8e6 Technologies

8e6® R3000 | Internet Filter

QUICK START GUIDE

Model: R3000IR

MSA-002-003

R3000 Release: 2.1.10, ER Release: 4.1.20 / Updated: 12.01.08

8E6 INTERNET FILTER WITH INTEGRATED REPORTER QUICK START GUIDE

© 2008 8e6 Technologies. All rights reserved.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

The R3000IR product has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# R3000IRul-QSG-081201

CONTENTS

R3000IR INTRODUCTION 1
About this Document 2
Conventions Used in this Document 3
SERVICE INFORMATION 4
PRELIMINARY SETUP PROCEDURES 5
Unpack the Unit from the Carton 5
Select a Site for the Server 6
Rack Mount the Server 6
Check the Power Supply 16
General Safety Information 17
INSTALL THE SERVER 20
Step 1: Setup Procedures 20
Step 1A: Quick Start Setup Procedures 21
Step 1B: Console Setup Procedures 29
Step 2: Test the R3000 Console Connection 41
Step 3: Test Filtering or Mobile Client Console Connection 42
Step 4: Set Library Updates 43
Step 5: Change the ER Admin User Name and Password, Set Self-Monitoring 47
Step 6: Client Workstation Configuration 50
Step 7: Launch the ER Client 51
CONCLUSION 53
BEST FILTERING PRACTICES 54
Threat Class Groups 54
Filtering Scenarios 55
IMPORTANT INFORMATION ABOUT USING THE ER IN THE EVALUATION MODE 71
Administrator Console, Expiration Screen 71
ER Client, ER Server Statistics Window 72

LED INDICATORS AND BUTTONS........73
Diagrams and Descriptions........73
REGULATORY SPECIFICATIONS AND DISCLAIMERS........74
Declaration of the Manufacturer or Importer........74
INDEX........77

R3000IR INTRODUCTION

Thank you for choosing to evaluate the 8e6 Technologies R3000IR Internet Filter with Integrated Reporter. This product combines the R3000 Internet Filter with the ER Enterprise Reporter to track end user Internet activity and generate reports that assist administrators in developing policies and targeting sites to be filtered, in order to maximize bandwidth utilization and productivity.

The R3000 can be configured to block specific Web sites or service ports, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources. This product also features expansive library categories, instant message and peer-to-peer blocking, user authentication, and intuitive screens and fields for ease of use when configuring and maintaining the server, as well as managing user and group filtering profiles.

The ER is comprised of the server and client application. Once the ER server is configured and R3000 log files have populated the database, an administrator can use the ER client reporting application to virtually generate an unlimited number of queries and reports from data in the database. This data shows which end user is accessing which site, the duration of each site visit, and the frequency of these visits. The client gives the administrator the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained, and then memorize and save the view to a user-defined report menu for repetitive, scheduled execution and distribution.

Quick setup procedures—to implement the best filtering practices for the scenarios described in the second paragraph—are included in the Best Filtering Practices section that follows the Conclusion of this guide.

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the R3000IR product and how to use this document
- **Service Information** - This section provides 8e6 Technologies contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to physically set up the R3000IR in your network environment
- **Install the Server** - This section explains how to configure the R3000IR for filtering and reporting
- **Conclusion** - This section indicates that the quick start steps have been completed
- **Best Filtering Practices** - This section includes a chart of library categories organized into Threat Class Groups, accompanied by filtering scenarios and directions for implementing the best filtering practices to secure your network, prevent excessive bandwidth usage, and increase productivity
- **Evaluation Mode** - This section gives information on using the ER in the evaluation mode
- **LED Indicators and Buttons** - This section explains how to read LED indicators and use LED buttons for troubleshooting the unit
- **Regulatory Specifications and Disclaimers** - This section cites safety and emissions compliance information for the R3000IR model referenced in this document
- **Index** - An alphabetized list of some topics included in this document

Conventions Used in this Document

The following icons are used throughout this document to call attention to important information pertaining to handling, operation, and maintenance of the server; safety and preservation of the equipment, and personal safety:

***NOTE:** The "note" icon is followed by additional information to be considered.*

***WARNING:** The "warning" icon is followed by information alerting you to a potential situation that may cause damage to property or equipment.*

***CAUTION:** The "caution" icon is followed by information warning you that a situation has the potential to cause bodily harm or death.*

***IMPORTANT:** The "important" icon is followed by information 8e6 recommends that you review before proceeding with the next action.*

The "book" icon references the R3000 User Guide. This icon is found in the Best Filtering Practices section of this document.

SERVICE INFORMATION

The user should not attempt any maintenance or service on the unit beyond the procedures outlined in this document.

Any initial hardware setup problem that cannot be resolved at your internal organization should be referred to an 8e6 Technologies solutions engineer or technical support representative.

8e6 Corporate Headquarters (USA)

Local	:	714.282.6111
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

8e6 Taiwan

Taipei Local	:	2397-0300
Domestic Taiwan	:	02-2397-0300
International	:	886-2-2397-0300

Procedures

When calling 8e6 Technologies regarding a problem, please provide the representative the following information:

- Your contact information.
- Serial number or original order number.
- Description of the problem.
- Network environment in which the unit is used.
- State of the unit before the problem occurred.
- Frequency and repeatability of the problem.
- Can the product continue to operate with this problem?
- Can you identify anything that may have caused the problem?

PRELIMINARY SETUP PROCEDURES

Unpack the Unit from the Carton

Inspect the packaging container for evidence of mishandling during transit. If the packaging container is damaged, photograph it for reference.

Carefully unpack the unit from the carton and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to 8e6 Technologies.

The carton should contain the following items:

- 1 R3000IR unit
- 1 AC Power Cord
- 1 Serial Port Cable
- 1 CAT-5E Crossover Cable
- 1 End User License Agreement (EULA)
- 1 envelope containing a CD-ROM with PDFs of R3000IR versions of the R3000 User Guide, R3000 Authentication User Guide, and ER User Guide. The latest version of the R3000IR user guides can be obtained from our Web site. For the R3000 User Guide, go to: **http://www.8e6.com/docs/ir_r3000_r2.pdf**. For the R3000 Authentication User Guide, go to: **http://www.8e6.com/docs/ir_r3000_auth2.pdf**. For the ER User Guide, go to: **http://www.8e6.com/docs/ir_er4server.pdf**.

NOTES: *A coupler is included in the carton if a three-foot CAT-5E crossover cable is packaged with your unit instead of a 14-foot CAT-5E crossover cable. Rack mount brackets (2) also may be included for installing the unit in a rack.*

Inspect the server and accessories for damage. If the contents appear damaged, file a damage claim with the carrier immediately.

WARNING: *To avoid danger of suffocation, do not leave plastic bags used for packaging the server or any of its components in places where children or infants may play with them.*

Select a Site for the Server

The server operates reliably within normal office environmental limits. Select a site that meets the following criteria:

- Clean and relatively free of excess dust.
- Well-ventilated and away from sources of heat, with the ventilating openings on the server kept free of obstructions.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields and noise caused by electrical devices such as elevators, copy machines, air conditioners, large fans, large electric motors, radio and TV transmitters, and high-frequency security devices.
- Access space provided so the server power cord can be unplugged from the power supply or the wall outlet—this is the only way to remove the AC power cord from the server.
- Clearance provided for cooling and airflow: Approximately 30 inches (76.2 cm) in the back and 25 inches (63.5 cm) in the front.
- Located near a properly earthed, grounded, power outlet.

Rack Mount the Server

Rack Setup Precautions

⚠ Warning:

Before rack mounting the server, the physical environment should be set up to safely accommodate the server. Be sure that:

- The weight of all units in the rack is evenly distributed. Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- The rack will not tip over when the server is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the rack.
- For multiple rack installations, racks are coupled together.
- Reliable earthing of rack-mounted equipment is maintained at all times. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- A power cord will be long enough to fit into the server when properly mounted in the rack and will be able to supply power to the unit.
- The connection of the server to the power supply will not overload any circuits. Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- The server is only connected to a properly rated supply circuit. Reliable earthing (grounding) of rack-mounted equipment should be maintained.
- The air flow through the server’s fan or vents is not restricted. Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- The maximum operating ambient temperature does not exceed 104°F (40°C). If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

⚠ ***WARNING:*** *Extend only one component at a time. Extending two or more components simultaneously may cause the rack to become unstable.*

Rack Mount Instructions

Optional: Install the Chassis Rails

NOTE: *If your chassis does not come with chassis rails, please follow the procedure listed on the last page of this sub-section to install the unit directly into the rack.*

CAUTION: *Please make sure that the chassis covers and chassis rails are installed on the chassis before you install the chassis into the rack. To avoid personal injury and property damage, please carefully follow all the safety steps listed below:*

Before installing the chassis rails:

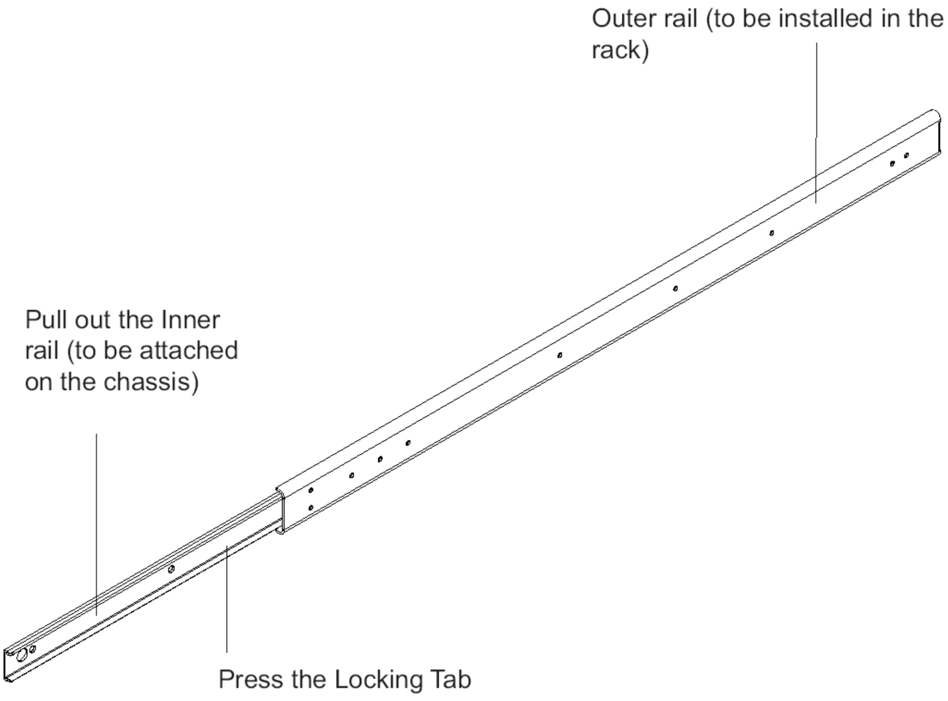
- *Close the chassis using the chassis cover.*
- *Unplug the AC power cord(s).*
- *Remove all external devices and connectors.*

---

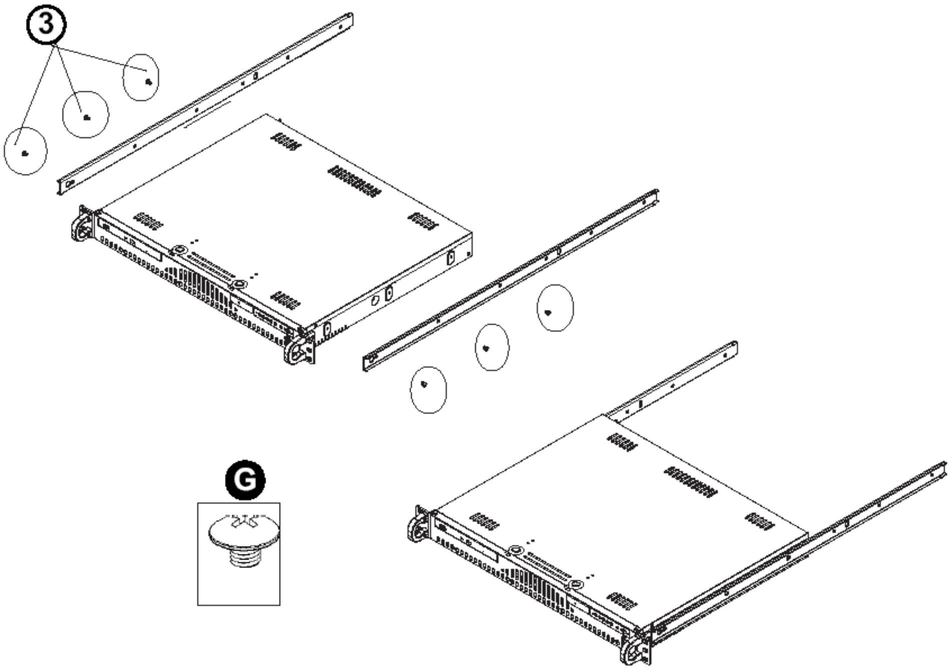
1. Included in the shipping package are a pair of rail assemblies. In each rail assembly, locate the inner rail and the outer rail.

2. Press the locking tab to release the inner rail from its locking position and pull out the inner rail from the rail assembly.

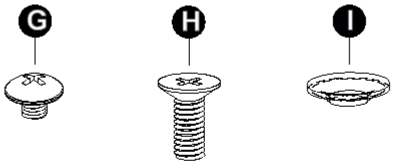
NOTE: *The inner rails are to be attached to the chassis and the outer rails are to be installed in the rack.*


Outer rail (to be installed in the rack)
Pull out the Inner rail (to be attached on the chassis)
Press the Locking Tab

3. Locate the three holes on each side of the chassis and locate the three corresponding holes on each of the inner rail.



4. Attach an inner rail to each side of the chassis and secure the inner rail to the chassis by inserting three Type G screws through the holes on each side of the chassis and the inner rail. (See the diagram below for a description of the Type G screw.)



G. Round head M4 x 4 mm [0.157]

H. Flat head M5 x 12 mm [0.472]

I. Washer for M5

5. Repeat the above steps to install the other rail on the chassis.

Optional: Install the Traditional UP Racks

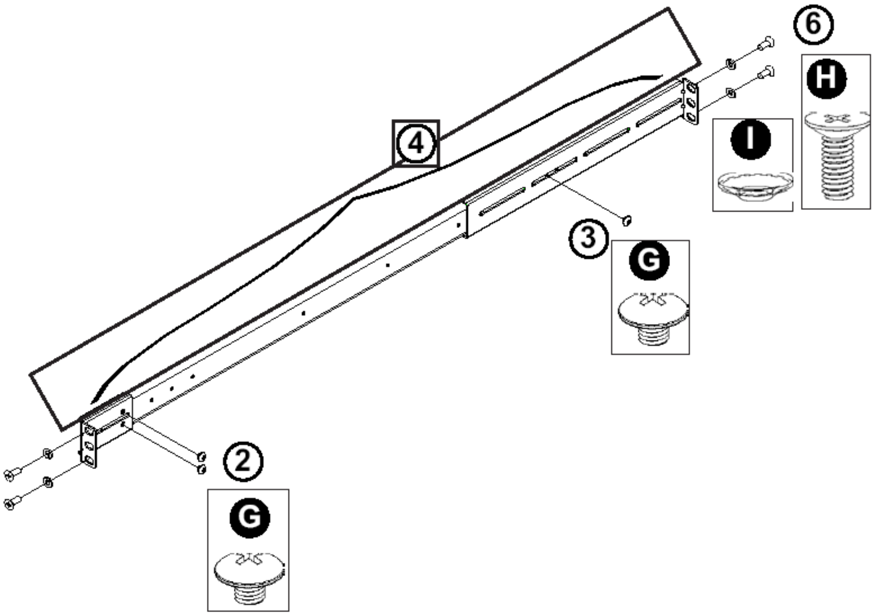
After you have installed the inner rails on the chassis, you are ready to install the outer rails of rail assemblies to the rack.

NOTE: *The rails are designed to fit in the racks with the depth of 28” to 33”.*

- *Determine the placement of each component in the rack before you install the rails.*
- *Install the heaviest server components on the bottom of the rack first, and then work up.*

---

1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).
2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws. (See the previous page for a description of the Type G screw.)
3. Attach the rear (long) bracket to the other end of the outer rail and secure the rear (long) bracket to the outer rail with a Type G screw as shown below.
4. Measure the depth of your rack and adjust the length of the rails accordingly.
5. Repeat the same steps to install the other outer rail on the chassis.
6. Secure both outer rail assemblies to the rack with Type H screws and Type I washers. (See the previous page for descriptions of Type H and Type I hardware components.)



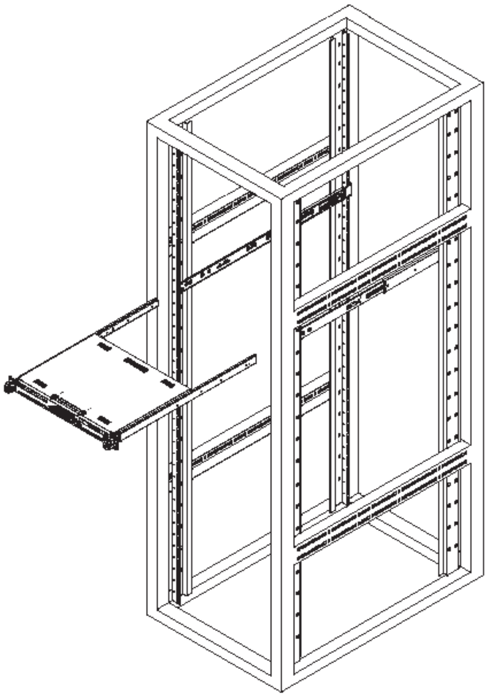
7. Slide the chassis into the rack as shown below.

NOTE: *The chassis may not slide into the rack smoothly or easily when installed the first time. Some adjustment to the slide assemblies might be needed for easy installation.*

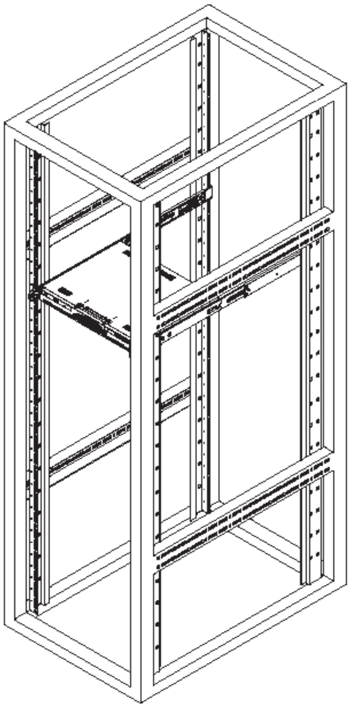
---

8. You will need to release the safety taps on both sides of the chassis in order to completely remove the chassis out of the rack.

7a



7b



Optional: Install the Open Racks

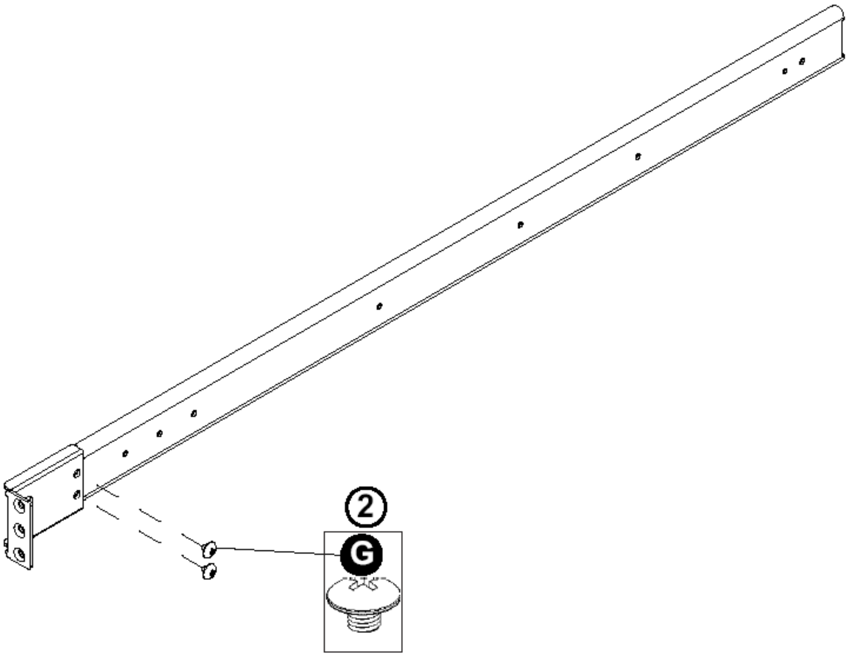
After you have installed the inner rails on the chassis, you are ready to install the outer rails of rail assemblies to the rack.

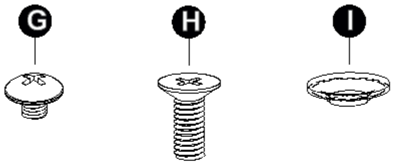
NOTE: *The rails are designed to fit in the racks with the depth of 28" to 33".*

- *Determine the placement of each component in the rack before you install the rails.*
- *Install the heaviest server components on the bottom of the rack first, and then work up.*

---

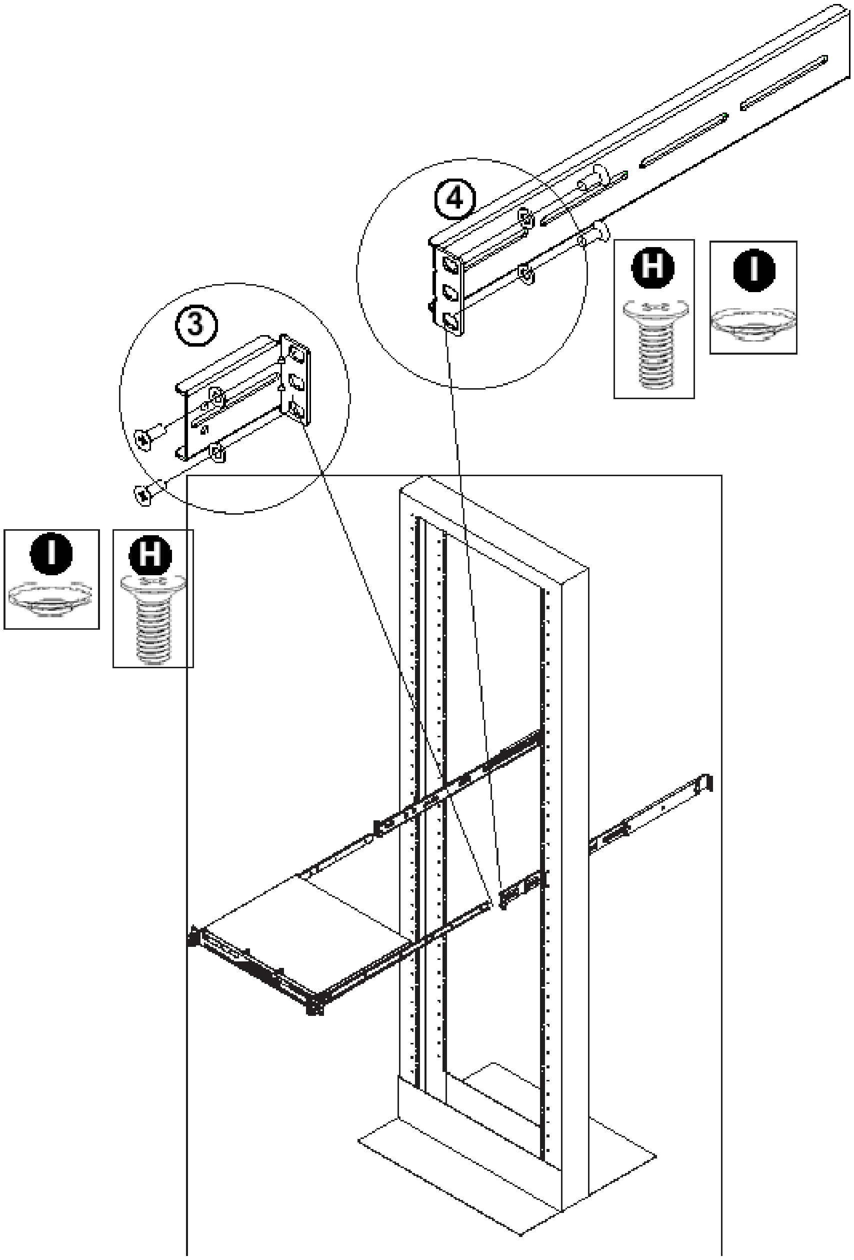
1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).
2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws as shown below.



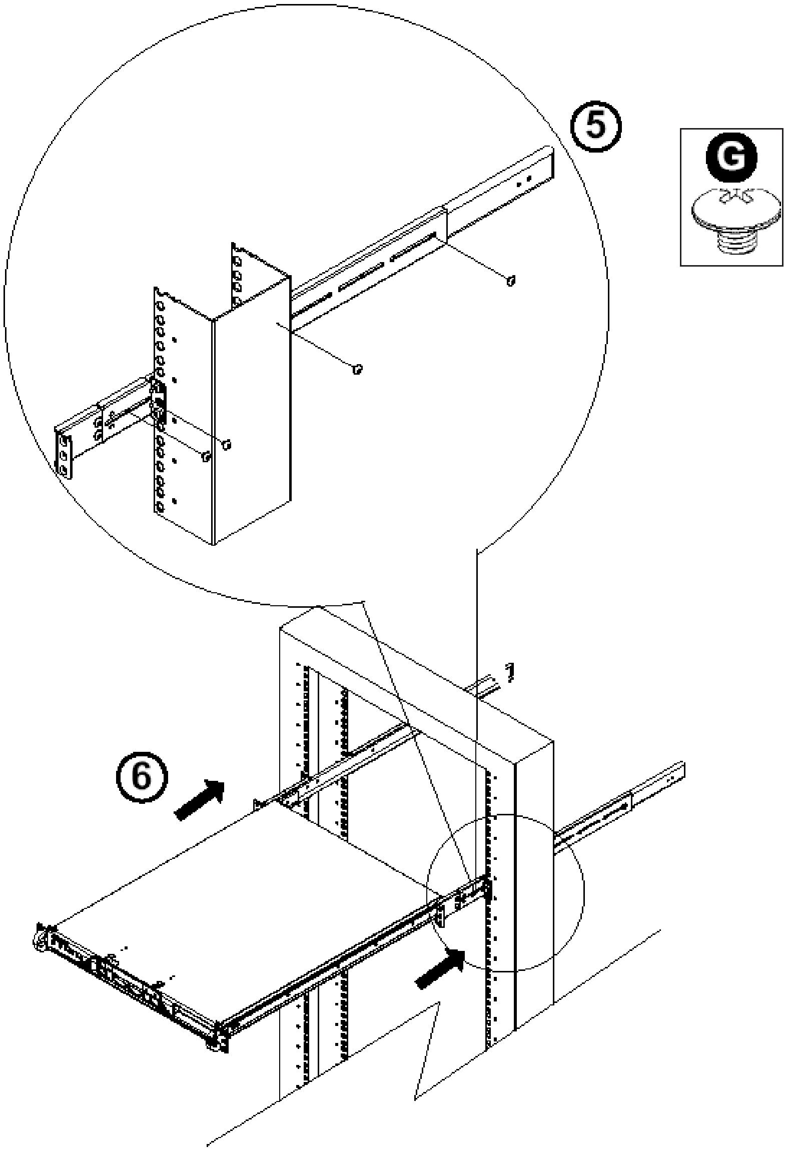


G. Round head M4 x 4 mm [0.157]
H. Flat head M5 x 12 mm [0.472]
I. Washer for M5

3. Attach the front (short) bracket to the front end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. (See the previous page for descriptions of Type H and Type I hardware components.)
4. Attach the rear (long) bracket to the rear end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. Repeat the same steps to install the other outer rail to the other side of rack.



5. Measure the depth of your rack and adjust the length of the rails accordingly. Then, secure the rails to the chassis with Type G screws.
6. Slide the inner rails which are attached to the chassis into the outer rails on the rack.

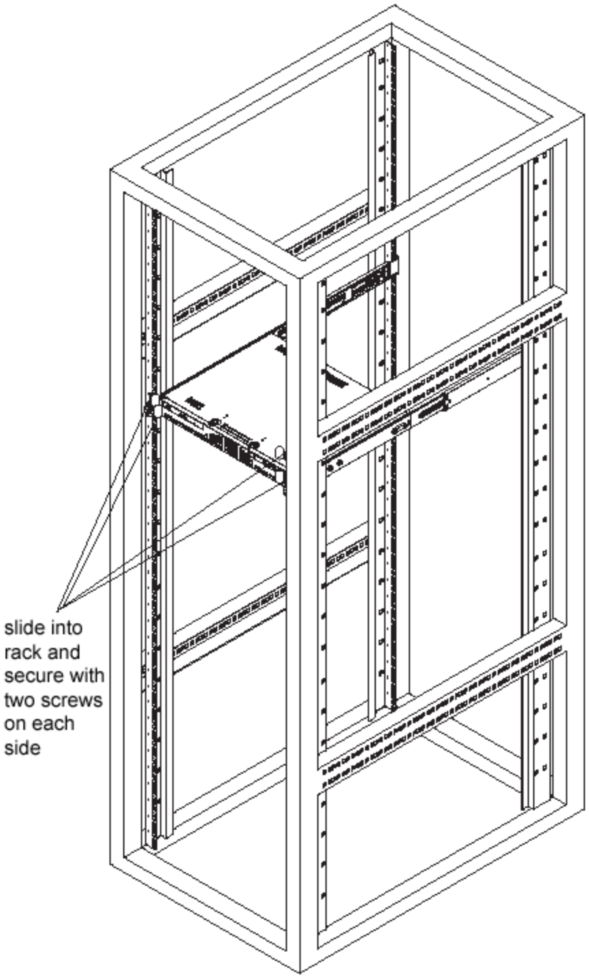


Install the Chassis into the Rack

CAUTION: *Before installing the chassis into the rack:*

- *Make sure that the rack is securely anchored onto an unmovable surface or structure before installing the chassis into the rack.*
- *Unplug power cord(s) of the rack before installing the chassis into the rack.*
- *Make sure that the system is adequately supported. Make sure that all the components are securely fastened to the chassis to prevent components falling off from the chassis.*
- *The rack assembly should be properly grounded to avoid electric shock.*
- *The rack assembly must provide sufficient airflow to the chassis for proper cooling.*
- *Please make sure that all components and all chassis covers are properly installed in the chassis before you install the chassis into the racks; otherwise, out-of-warranty damage may occur.*

Slide the chassis into the rack and secure it with two screws on each side of the rack as shown in the picture.



Check the Power Supply

This server is equipped with a universal power supply that handles 100-240 V, 50/60 Hz. A standard power cord interface (IEC 950) facilitates power plugs that are suitable for most European, North American, and Pacific Rim countries.

Power Supply Precautions

⚠ **Warning:**

- Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep the server operating in case of a power failure.
- In geographic regions that are susceptible to electrical storms, 8e6 highly recommends plugging the AC power cord for the server into a surge suppressor.
- Use appropriately rated extension cords or power strips only.
- Allow power supply units to cool before touching them.

General Safety Information

Server Operation and Maintenance Precautions

⚠ Warning:

Observe the following safety precautions during server operation and maintenance:

⚠ ***WARNING:*** *If the server is used in a manner not specified by the manufacturer, the protection provided by the server may be impaired.*

⚠ ***WARNING:*** *8e6 Technologies is not responsible for regulatory compliance of any server that has been modified. Altering the server's enclosure in any way other than the installation operations specified in this document may invalidate the server's safety certifications.*

☠ ***CAUTION:*** *Never pile books, papers, or other objects on the chassis, drop it, or subject it to pressure in any other way. The internal circuits can be damaged, and the battery may be crushed or punctured. Besides irreparable damage to the unit, the result could be dangerous heat and even fire.*

☠ ***CAUTION:*** *There are no user-serviceable components inside the chassis. The chassis should only be opened by qualified service personnel. Never disassemble, tamper with, or attempt to repair the server. Doing so may cause smoke, fire, electrical shock, serious physical injury, or death.*

- Do not insert objects through openings in the chassis. Doing so could result in a short circuit that might cause a fire or an electrical shock.
- Do not operate the server in an explosive atmosphere, in the presence of flammable gases.
- To ensure proper cooling, always operate the server with its covers in place. Do not block any openings on the chassis. Do not place the server near a heater.
- Always exit the software application properly before turning off the server to ensure data integrity.
- Do not expose the server to rain or use near water. If liquids of any kind should leak into the chassis, power down the server, unplug it, and contact 8e6 Technologies technical support.
- Disconnect power from the server before cleaning the unit. Do not use liquid or aerosol cleaners.

AC Power Cord and Cable Precautions

Warning:

- The AC power cord for the server must be plugged into a grounded, power outlet.
- Do not modify or use a supplied AC power cord if it is not the exact type required in the region where the server will be installed and used. Replace the cord with the correct type.
- Route the AC power cord and cables away from moving parts and foot traffic.
- Do not allow anything to rest on the AC power cord and cables.
- Never use the server if the AC power cord has been damaged.
- Always unplug the AC power cord before removing the unit for servicing.

Electrical Safety Precautions

Warning:

Heed the following safety precautions to protect yourself from harm and the server from damage:

***CAUTION:** Dangerous voltages associated with the 100-240 V AC power supply are present inside the unit. To avoid injury or electrical shock, do not touch exposed connections or components while the power is on.*

- To prevent damage to the server, read the information in this document for selection of the proper input voltage.
- Do not wear rings or wristwatches when troubleshooting electrical circuits.
- To avoid fire hazard, use only the specified fuse(s) with the correct type number, voltage, and current ratings. Only qualified service personnel should replace fuses.
- Qualified service personnel should be properly grounded when servicing the unit.
- Qualified service personnel should perform a safety check after any service is performed.

Motherboard Battery Precautions

Caution:

The battery on the motherboard should not be replaced without following instructions provided by the manufacturer. Only qualified service personnel should replace batteries.

The battery contains energy and, as with all batteries, a malfunction can cause heat, smoke, or fire, release toxic materials, or cause burns. Do not disassemble, puncture, drop, crush, bend, deform, submerge or modify the battery. Do not incinerate or expose to heat above 140°F (60°C).

There is a danger of explosion if the battery on the motherboard is installed upside down, which will reverse its polarities.

CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISPOSE OF THE USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

ATTENTION: IL Y A DANGER D'EXPLOSION S'IL Y A REPLACEMENT INCORRECT DE LA BATTERIE, REMPLACER UNIQUEMENT AVEC UNE BATTERIE DU MÊME TYPE OU D'UN TYPE ÉQUIVALENT RECOMMANDÉ PAR LE CONSTRUCTEUR. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÊMENT AUX INSTRUCTIONS DU FABRICANT.

WARNING: *Users in Member States should consult Article 20 of Directive 2006/66/EC of the European Parliament and of the Council before disposing the motherboard battery.*

INSTALL THE SERVER

Step 1: Setup Procedures

This step requires you to link the workstation to the R3000IR. You have the option of using the text-based Quick Start setup procedures described in Step 1A, or the Administrator console setup procedures described in Step 1B.

Quick Start Setup Requirements

The following hardware is required for the Quick Start setup procedures:

- R3000IR with AC power cord
- either one of two options:
    - PC monitor with AC power cord and keyboard, or
    - PC laptop computer with HyperTerminal and serial port cable (and USB DB9 serial adapter, if there is no serial port on your laptop)

Go to Step 1A to execute Quick Start Setup Procedures.

Administrator Console Setup Requirements

The following hardware is required for the Administrator console setup procedures:

- R3000IR unit with AC power cord
- CAT-5E crossover cable
- PC laptop computer, or PC monitor with AC power cord and keyboard

Go to Step 1B to execute Console Setup Procedures.

Step 1A: Quick Start Setup Procedures

Link the Workstation to the R3000IR

Monitor and Keyboard Setup

A. Connect the PC monitor and keyboard cables to the rear of the chassis (see Fig. 1).

B. Turn on the PC monitor.

C. Power on the R3000IR by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 2).

Once the R3000IR is powered up, proceed to the Login screen instructions.

Serial Console Setup

A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see Fig. 1).

B. Power on the laptop.

C. Power on the R3000IR by pressing the large button on the front panel (see Fig. 2).

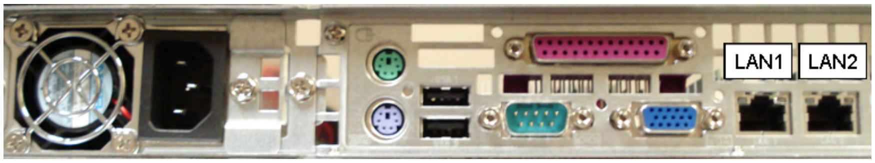


Fig. 1 - Portion of MSA chassis rear

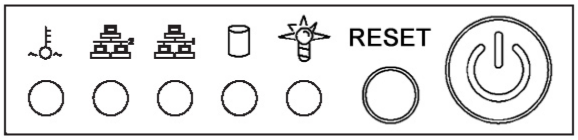


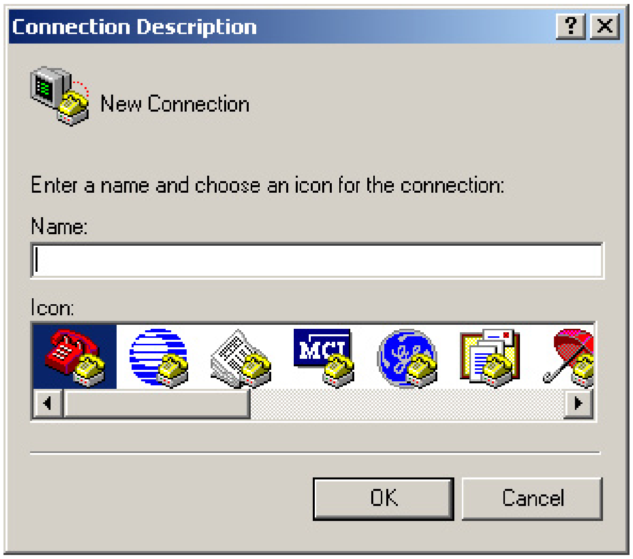
Fig. 2 - Diagram of MSA chassis front panel, power button at far right

Once the R3000IR is powered up, proceed to the instructions for HyperTerminal Setup Procedures.

HyperTerminal Setup Procedures

If using a serial console, follow these procedures to create a HyperTerminal session.

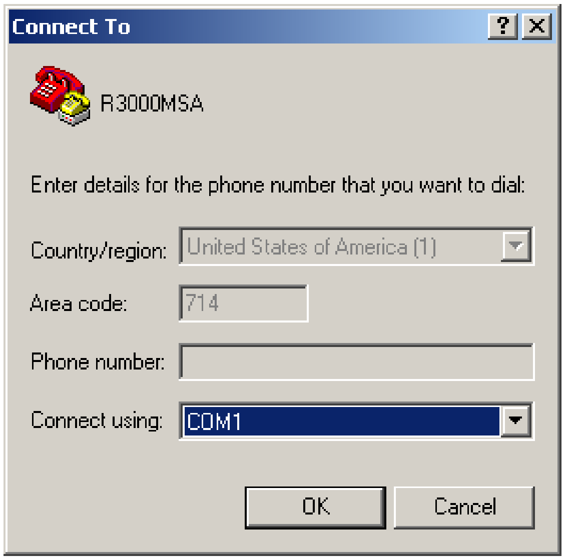
A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



Enter a name and choose an icon for the connection:

Name:

B. In the Connection Description dialog box, enter any session **Name**, and then click **OK** to open the Connect To dialog box:



R3000MSA

Enter details for the phone number that you want to dial:

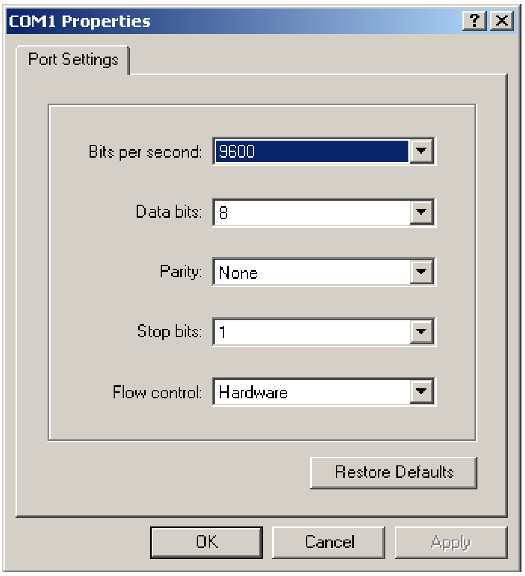
Country/region: United States of America (1)

Area code: 714

Phone number:

Connect using: COM1

C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

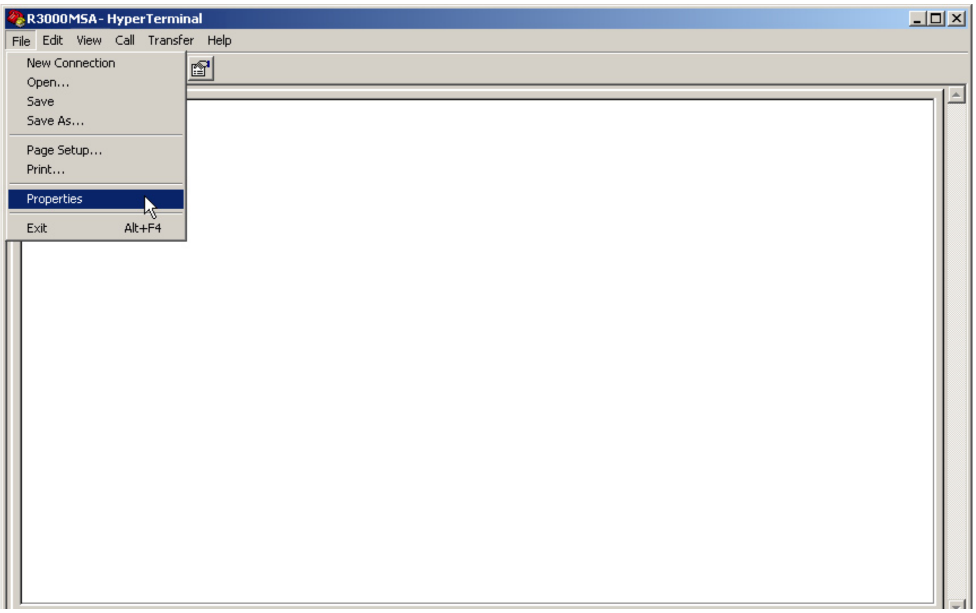
Flow control: Hardware

Restore Defaults
OK
Cancel
Apply

D. Specify the following session settings:

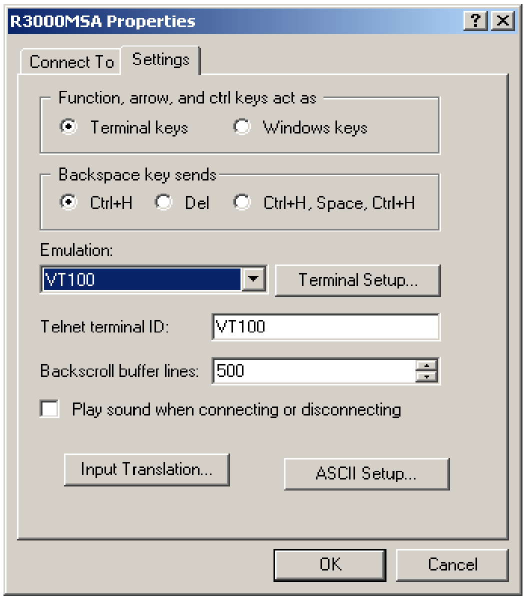
- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware

E. Click **OK** to connect to the HyperTerminal session:



R3000MSA - HyperTerminal
File
Edit
View
Call
Transfer
Help
New Connection
Open…
Save
Save As…
Page Setup…
Print…
Properties
Exit
Alt+F4

F. In the HyperTerminal session window, go to File > Properties to open the Properties dialog box, displaying the Connect To and Settings tabs:



R3000MSA Properties

Function, arrow, and ctrl keys act as: ● Terminal keys ○ Windows keys

Backspace key sends: ● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

☐ Play sound when connecting or disconnecting

?
Connect To
Settings
Terminal Setup...
Input Translation...
ASCII Setup...
OK
Cancel

G. Click the Settings tab, and at the **Emulation** menu select “VT100”.

H. Click **OK** to close the dialog box, and to go to the login screen.

NOTE: *If using a HyperTerminal session, the login screen will display with black text on a white background.*

Login screen

The login screen displays after powering on the R3000IR unit using a monitor and keyboard, or after creating a HyperTerminal session.

---

*NOTE: If the screensaver currently displays on your screen, press the **Enter** key to display the login screen.*

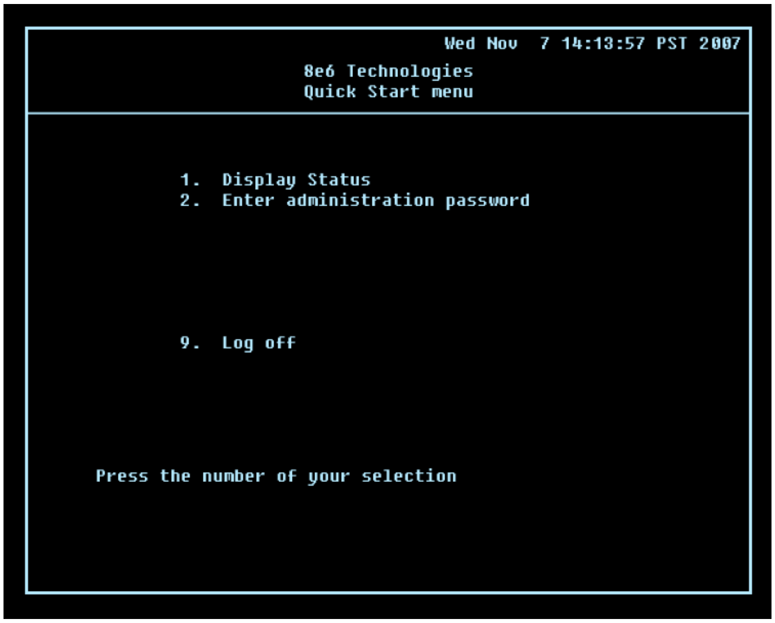
A. At the **login** prompt, type in ***menu***.

B. Press the **Enter** key to display the Password prompt.

C. At the **Password** prompt, type in the following: ***#s3tup#r3k***

D. Press **Enter** to display the Quick Start menu screen.

Quick Start menu screen



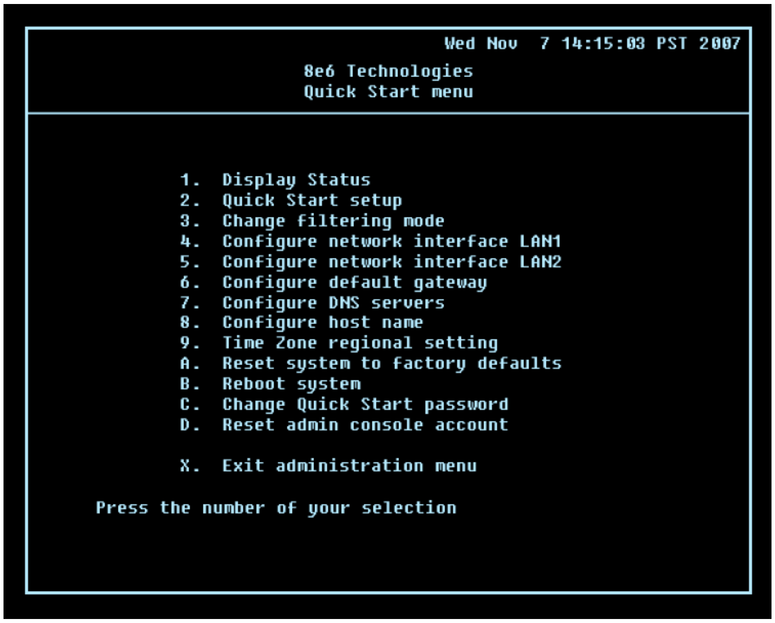
```
                                         Wed Nov  7 14:13:57 PST 2007
                          8e6 Technologies
                          Quick Start menu

            1.  Display Status
            2.  Enter administration password




            9.  Log off




    Press the number of your selection
```

A. At the **Press the number of your selection** prompt, press **2** to select the Quick Start setup process.

B. At the login prompt, re-enter your password: ***#s3tup#r3k***

C. Press **Enter** to display the administration menu where you can begin using the Quick Start setup procedures.

Quick Start menu: administration menu



```
                                         Wed Nov  7 14:15:03 PST 2007
                         8e6 Technologies
                         Quick Start menu

              1.  Display Status
              2.  Quick Start setup
              3.  Change filtering mode
              4.  Configure network interface LAN1
              5.  Configure network interface LAN2
              6.  Configure default gateway
              7.  Configure DNS servers
              8.  Configure host name
              9.  Time Zone regional setting
              A.  Reset system to factory defaults
              B.  Reboot system
              C.  Change Quick Start password
              D.  Reset admin console account

              X.  Exit administration menu

      Press the number of your selection
```

A. At the **Press the number of your selection** prompt, press **2** to select the “Quick Start Setup” process.

The Quick Start menu takes you to the following configuration screens to make entries for configuring the R3000:

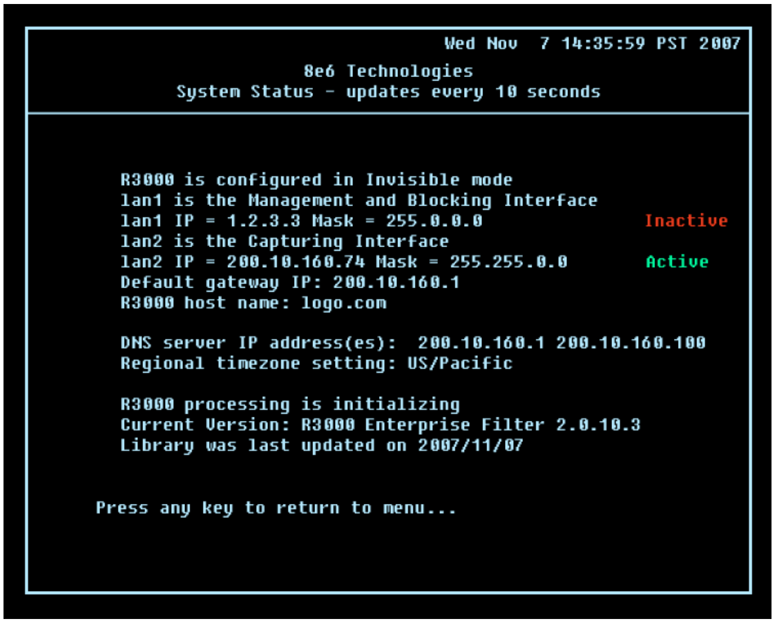
- Change filtering mode
- Configure network interface LAN1
- Configure network interface LAN2
- Configure default gateway
- Configure DNS servers
- Configure host name
- Time Zone regional setting

NOTE: *See the Network screens for Operation Mode, LAN Settings, and Regional Setting in Step 1B for content included in the Quick Start setup screens.*

B. After making all entries using the Quick Start setup procedures, press **X** to return to the Quick Start menu screen. Or, to verify the status of the R3000 and review the entries you made using the Quick Start setup, press **1** to view the System Status screen.

NOTES: *Changing your password using option C, “Change Quick Start password”, will change the password for the console menu but not the R3000 console login screen. Option A, “Reset system to factory defaults”, should only be used by an 8e6 Technologies technical representative. Option D, “Reset admin console account”, should be used for resetting the administrator console username and password to the factory default ‘admin’/’user3’ and for unlocking all IP addresses currently locked.*

System Status screen



```
                                        Wed Nov  7 14:35:59 PST 2007
                            8e6 Technologies
                   System Status - updates every 10 seconds


        R3000 is configured in Invisible mode
        lan1 is the Management and Blocking Interface
        lan1 IP = 1.2.3.3 Mask = 255.0.0.0                  Inactive
        lan2 is the Capturing Interface
        lan2 IP = 200.10.160.74 Mask = 255.255.0.0          Active
        Default gateway IP: 200.10.160.1
        R3000 host name: logo.com

        DNS server IP address(es):  200.10.160.1 200.10.160.100
        Regional timezone setting: US/Pacific

        R3000 processing is initializing
        Current Version: R3000 Enterprise Filter 2.0.10.3
        Library was last updated on 2007/11/07


      Press any key to return to menu...
```

The System Status screen contains the following information:

- **Operation Mode** specified in screen 3 (Change filter mode)
- **Management and Blocking Interface** specified in screen 4 or 5 (Configure network interface LAN1 or LAN2)
- **Capturing Interface** specified in screen 4 or 5 (Configure network interface LAN1 or LAN2)
- **lan1 IP** address and netmask specified in screen 4, and current status (“Active” or “Inactive”)
- **lan2 IP** address and netmask specified in screen 5, and current status (“Active” or “Inactive”)
- **Default gateway** IP address specified in screen 6 (Configure default gateway)
- **R3000 host name** specified in screen 8 (Configure host name)
- **DNS server IP address(es)** specified in screen 7 (Configure DNS servers)
- **Regional timezone setting** specified in screen 9 (Time Zone regional setting)
- Current status of the R3000
- Current R3000 software **Version** installed
- Library update status

NOTE: *Modifications can be made at any time by returning to the specific screen of the Quick Start procedures.*

Log Off, Disconnect the Peripherals

A. After completing the Quick Start setup procedures, return to the Quick Start menu screen and press **9** to log out.

B. Disconnect the peripherals from the R3000IR.

Step 1B: Console Setup Procedures

Preliminary Setup

Create a “setup workstation” using a Windows-based laptop or desktop machine with a network card and Internet Explorer 5.5 (or later). The setup workstation will be used for accessing the R3000 Administrator console on the network and configuring the server.

NOTE: *The Java Plug-in version specified for the R3000 software version must be installed on your workstation. If your workstation does not have Java Runtime Environment, you will be prompted to install it.*

Workstation Configurations

A. From the desktop of the setup workstation, follow the procedures for your machine type:

- **Windows XP** - go to Start > Control Panel. Open Network Connections. Right-click the link for LAN or High-Speed Internet and choose Properties.
- **Windows 2000** - right-click the My Network Places icon and select Properties. Right-click the correct Local Area Connection and choose Properties.
- **Windows NT** - right-click the Network Neighborhood icon and select Properties.
- **Windows ME** - right-click the My Network Places icon and select Properties.

B. Click on **Internet Protocol (TCP/IP)** to highlight it (Windows NT and ME users should select the Protocols or Configuration tab and choose **TCP/IP Protocol**).

C. Click the **Properties** button.

⚠ ***WARNING:*** *Be sure to make note of the current network settings on the setup workstation as you will need to return them for further setup procedures.*

D. Choose the option **Use the following IP address** (Windows NT and ME users should choose the option **Specify an IP Address**).

E. Type in the **IP address** of 1.2.3.1.

F. Type in the **Subnet mask** (netmask) of 255.0.0.0 and click **OK**.

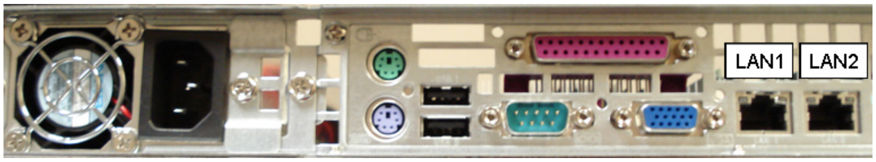
G. Close the LAN connection properties box.

Link the Workstation to the R3000IR

The procedures outlined in this sub-section require the use of the CAT-5E crossover cable.

A. Plug one end of the CAT-5E crossover cable into the R3000IR’s **LAN 2** port.

NOTE: *When facing the rear of the chassis, the LAN 2 port is the port on the right.*



Portion of MSA chassis rear

B. Plug the other end of the CAT-5E crossover cable into the setup workstation’s network card.

NOTE: *If you have a CAT-5E coupler, this can be used if the crossover cable is not long enough for your setup. Plug one end of the CAT-5E crossover cable into the R3000, and the other end into the coupler. Plug a standard CAT-5E cable into the other end of the coupler, and the free end of the standard CAT-5E cable into the setup workstation.*

C. Plug the R3000IR into a power source with an appropriate rating.

WARNING: *It is strongly suggested you use an uninterruptible power supply.*

D. Power on the R3000IR by lowering the face plate and pressing the large button at the right of the front panel (see diagram below):

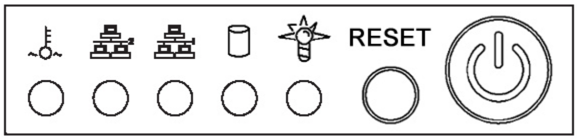


Diagram of MSA chassis front panel, power button at far right

The Boot Up Process

The boot-up process may take 5 - 10 minutes. When the drive light remains off for 30 seconds, the system is booted up. (See the LED Indicators and Buttons section for a description of front panel LED indicators and buttons.)

If you wish to verify that the unit has been booted up, you can perform the following test on your workstation:

1. Go to your taskbar and click Start > Run.
2. In the dialog box, type in ***cmd*** (type in ***command*** if using Windows ME).
3. Click **OK.**
4. In the cmd.exe window, type in ***ping 1.2.3.4***
5. Press **Enter** on your keyboard.

If you receive a reply, the unit is up.

Network Setup

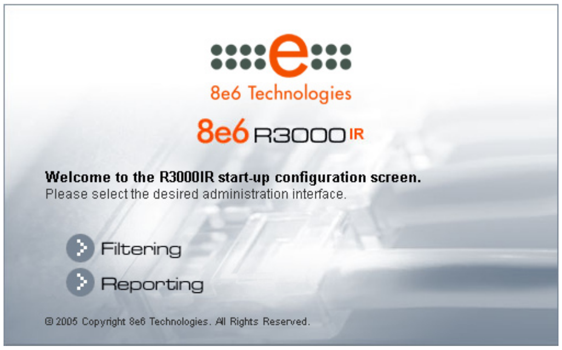
When the R3000IR is fully booted, you can configure network settings. For this step, you will need your network administrator to provide you the host name, gateway address, and two unused IP addresses. You will first configure the R3000 server and then configure the ER server.

Access the R3000IR Administrator Console

A. Launch Internet Explorer from the setup workstation.

B. Type in **http://1.2.3.4:88** in the address field.

C. Click **Go** to open the R3000IR console:

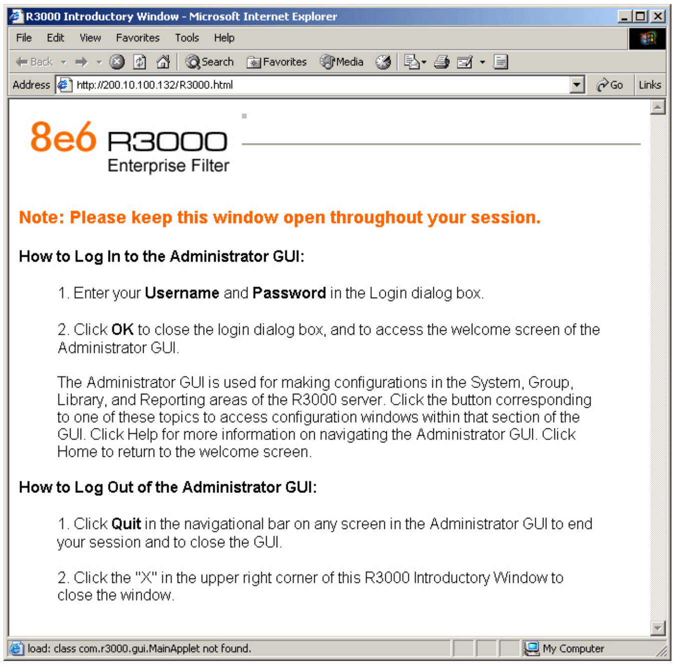


Welcome to the R3000IR start-up configuration screen.
Please select the desired administration interface.

© 2005 Copyright 8e6 Technologies. All Rights Reserved.

Log in to R3000 Administrator Console

A. In the console, click the link for **Filtering** to open the R3000 Introductory Window:


R3000 Introductory Window - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
http://200.10.100.132/R3000.html
Go
Links
8e6 R3000
Enterprise Filter
My Computer

Note: Please keep this window open throughout your session.

How to Log In to the Administrator GUI:

1. Enter your **Username** and **Password** in the Login dialog box.

2. Click **OK** to close the login dialog box, and to access the welcome screen of the Administrator GUI.

The Administrator GUI is used for making configurations in the System, Group, Library, and Reporting areas of the R3000 server. Click the button corresponding to one of these topics to access configuration windows within that section of the GUI. Click Help for more information on navigating the Administrator GUI. Click Home to return to the welcome screen.

How to Log Out of the Administrator GUI:

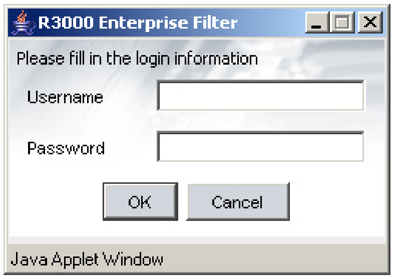
1. Click **Quit** in the navigational bar on any screen in the Administrator GUI to end your session and to close the GUI.

2. Click the "X" in the upper right corner of this R3000 Introductory Window to close the window.

load: class com.r3000.gui.MainApplet not found.

NOTE: *This window must be left open throughout your session.*

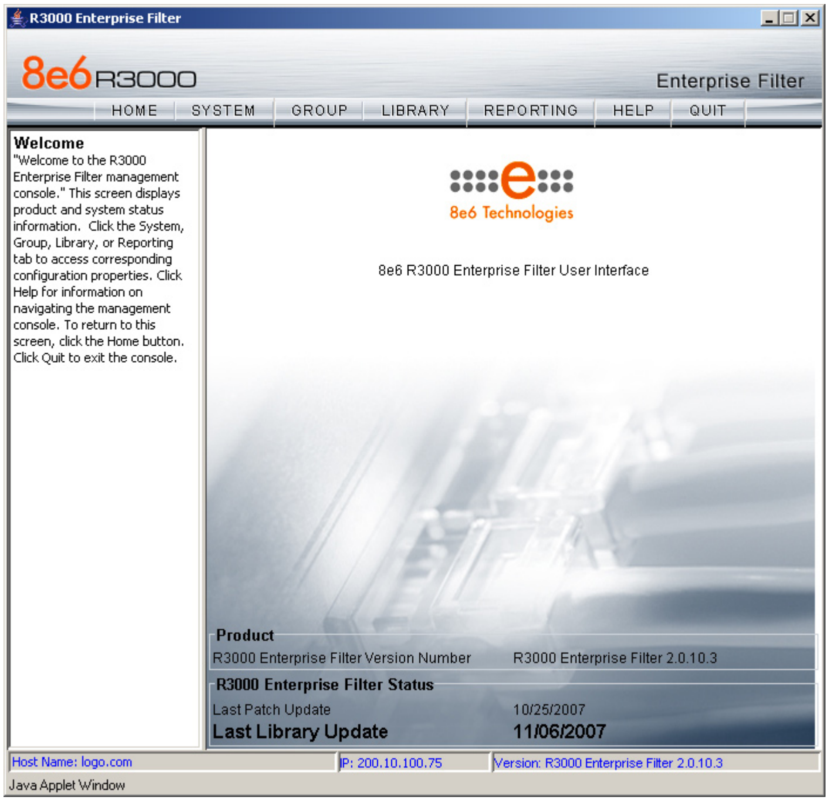
The Introductory Window displays minimized when the login dialog box of the R3000 Administrator console application opens:


R3000 Enterprise Filter
Please fill in the login information
Username
Password
OK
Cancel
Java Applet Window

B. In the **Username** field, type in ***admin***.

C. In the **Password** field, type in ***user3***.

D. Click **OK** to go to the main screen of the R3000 Administrator console:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
8e6 Technologies
8e6 R3000 Enterprise Filter User Interface
Java Applet Window

Welcome
"Welcome to the R3000 Enterprise Filter management console." This screen displays product and system status information. Click the System, Group, Library, or Reporting tab to access corresponding configuration properties. Click Help for information on navigating the management console. To return to this screen, click the Home button. Click Quit to exit the console.

Product

R3000 Enterprise Filter Version Number	R3000 Enterprise Filter 2.0.10.3

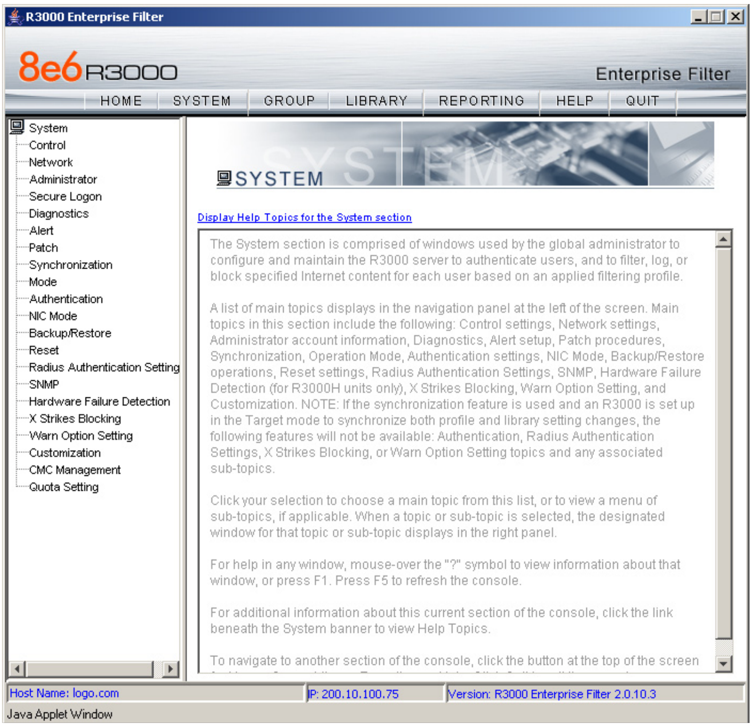
R3000 Enterprise Filter Status

Last Patch Update	10/25/2007
Last Library Update	**11/06/2007**

Host Name: logo.com | IP: 200.10.100.75 | Version: R3000 Enterprise Filter 2.0.10.3

Network

Click the **System** button at the top of the screen to go to the System section of the console:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
System
Control
Network
Administrator
Secure Logon
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Warn Option Setting
Customization
CMC Management
Quota Setting
SYSTEM
Display Help Topics for the System section
Java Applet Window

The System section is comprised of windows used by the global administrator to configure and maintain the R3000 server to authenticate users, and to filter, log, or block specified Internet content for each user based on an applied filtering profile.

A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include the following: Control settings, Network settings, Administrator account information, Diagnostics, Alert setup, Patch procedures, Synchronization, Operation Mode, Authentication settings, NIC Mode, Backup/Restore operations, Reset settings, Radius Authentication Settings, SNMP, Hardware Failure Detection (for R3000H units only), X Strikes Blocking, Warn Option Setting, and Customization. NOTE: If the synchronization feature is used and an R3000 is set up in the Target mode to synchronize both profile and library setting changes, the following features will not be available: Authentication, Radius Authentication Settings, X Strikes Blocking, or Warn Option Setting topics and any associated sub-topics.

Click your selection to choose a main topic from this list, or to view a menu of sub-topics, if applicable. When a topic or sub-topic is selected, the designated window for that topic or sub-topic displays in the right panel.

For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link beneath the System banner to view Help Topics.

To navigate to another section of the console, click the button at the top of the screen

Host Name: logo.com

IP: 200.10.100.75

Version: R3000 Enterprise Filter 2.0.10.3

In this section of the console you will:

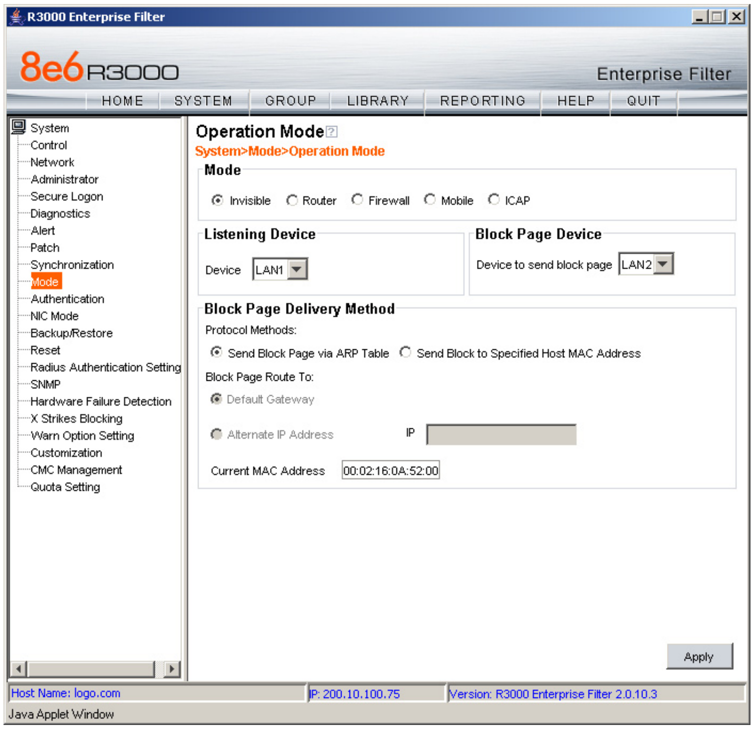
- Specify the operation mode the R3000 will use for filtering the network, listening to traffic, and sending traffic
- Configure LAN settings the R3000 will use on your network
- Select NTP servers the R3000 will use for time synchronization with Internet clocks
- Indicate the region in which the R3000 is geographically located

---

NOTE: *After saving your entries in each of these windows (Operation Mode, LAN Settings, NTP Servers, Regional Setting), you may be prompted to restart or reboot the server. Click* ***OK*** *to acknowledge the contents of the alert box, and then proceed to the next sub-step* ***without*** *restarting or rebooting the server.*

Network: Operation Mode

From the navigation panel at the left of the screen, click Mode and choose Operation Mode from the pop-up menu:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
System
Control
Network
Administrator
Secure Logon
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Warn Option Setting
Customization
CMC Management
Quota Setting
Apply
Java Applet Window

Operation Mode

System>Mode>Operation Mode

Mode

● Invisible ○ Router ○ Firewall ○ Mobile ○ ICAP

Listening Device

Device LAN1

Block Page Device

Device to send block page LAN2

Block Page Delivery Method

Protocol Methods:

● Send Block Page via ARP Table ○ Send Block to Specified Host MAC Address

Block Page Route To:

● Default Gateway

○ Alternate IP Address IP

Current MAC Address 00:02:16:0A:52:00

Host Name: logo.com IP: 200.10.100.75 Version: R3000 Enterprise Filter 2.0.10.3

Make the following entries in the Operation Mode window:

A. In the Mode frame, select the operational mode the R3000 will use for filtering: Invisible, Router, Firewall, Mobile, or ICAP.

NOTE: *Refer to the appendix in the R3000 User Guide for information on configuring the R3000 to use the Mobile mode option with the 8e6 Mobile Client.*

B. In the Listening Device frame, select the device for listening to traffic:

- **For the invisible mode**: “LAN1” is generally used as the default listening device
- **For the router or firewall mode**: Select the network card that will be used to “listen to”—as opposed to “send”—traffic on the network

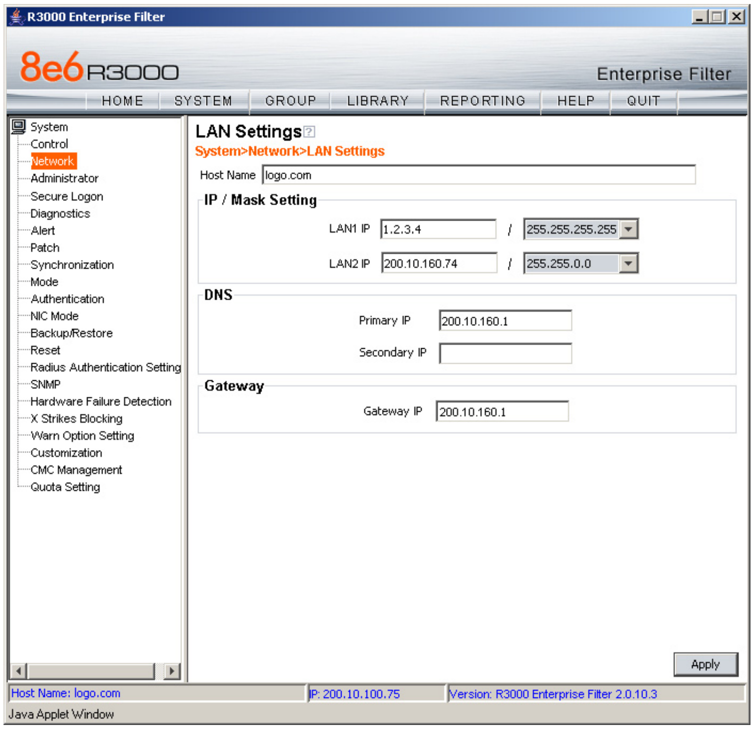
C. In the Block Page Device frame, select the device for sending block pages to client PCs:

- **For the invisible mode**: The block page device should be a different device than the one selected in the Listening Device frame—“LAN2” is generally used as the default device for sending block pages
- **For the router or firewall mode**: The device should be the same as the one selected in the Listening Device frame

D. Click **Apply**.

Network: LAN Settings

From the navigation panel, click Network and choose LAN Settings from the pop-up menu:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
System
Control
Network
Administrator
Secure Logon
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Warn Option Setting
Customization
CMC Management
Quota Setting
Apply
Java Applet Window

LAN Settings

System>Network>LAN Settings

Host Name: logo.com

IP / Mask Setting

LAN1 IP: 1.2.3.4 / 255.255.255.255

LAN2 IP: 200.10.160.74 / 255.255.0.0

DNS

Primary IP: 200.10.160.1

Secondary IP:

Gateway

Gateway IP: 200.10.160.1

Host Name: logo.com | IP: 200.10.100.75 | Version: R3000 Enterprise Filter 2.0.10.3

Make the following entries for the R3000 in the LAN Settings window:

A. Enter the **Host Name** that includes your domain name, for example R3000SERVER. myserver.com (the NetBIOS name must be capitalized). It is important to enter something identifiable, because once the product is registered, this host name is used by 8e6 Technologies to recognize your account for library updates. This name needs to be a valid DNS entry.

B. Enter the **LAN1 IP** address and specify the subnet for LAN 1, the R3000's first Ethernet Network Interface Card (NIC).

For the invisible mode, you may use a non-routeable IP address for the listening interface and a subnet mask of 255.255.255.255 (32 bites).

C. Enter the **LAN2 IP** address and subnet for LAN 2, the R3000's second Ethernet NIC. The subnet selection is usually 255.255.0.0 (16 bites) or 255.255.255.0 (24 bites), ***but cannot be 255.255.255.255 (32 bites)***.

For the router or firewall mode, the LAN 1 IP address should be in a different subnet than the LAN 2 IP address.

⚠ ***WARNING:*** *For the router and firewall mode, do not use the same subnet for LAN 1 and LAN 2 or the console will become inaccessible.*

D. Enter the **Primary IP** address of the first DNS name server. The R3000 uses this name server to resolve the domain name requested by users from the LAN.

E. Enter the **Secondary IP** address of the second DNS name server. The R3000 will use this name server to resolve the domain name requested by users from the LAN if the first DNS isn't working.

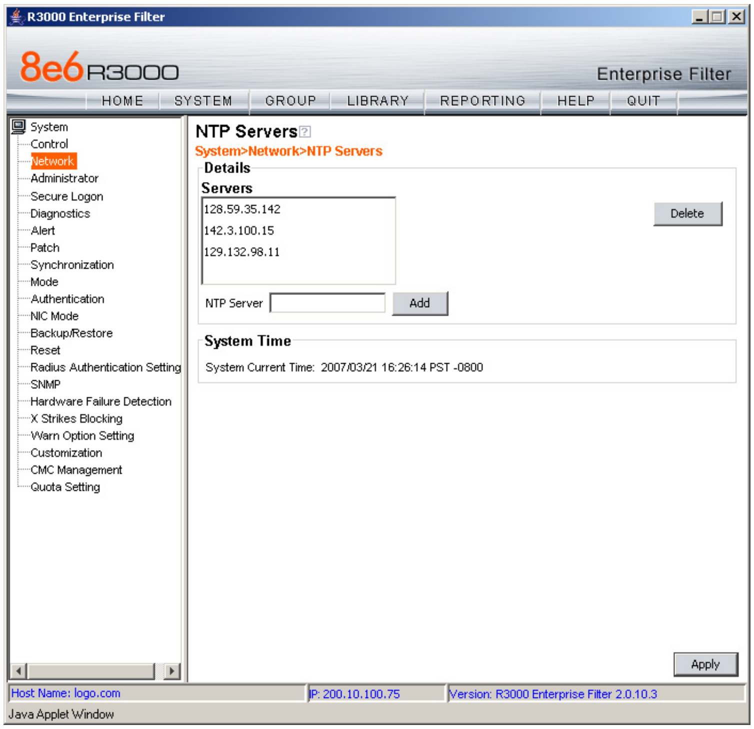
F. Enter the **Gateway IP** address for the default router or firewall that is the main gateway for the entire network. The R3000 will use this IP address to communicate outside the network.

⚠ ***WARNING: Be sure to take note of the LAN 1 and LAN 2 IP addresses and host name you assigned to the R3000. It is strongly suggested you document and store this information as it is now the only way of communicating with the R3000.***

G. Click **Apply**.

Network: NTP Servers

From the navigation panel, click Network and choose NTP Servers from the pop-up menu:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
System
Control
Network
Administrator
Secure Logon
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Warn Option Setting
Customization
CMC Management
Quota Setting
Delete
Add
Apply
Java Applet Window

NTP Servers

System>Network>NTP Servers

Details

Servers

128.59.35.142
142.3.100.15
129.132.98.11

NTP Server

System Time

System Current Time: 2007/03/21 16:26:14 PST -0800

Host Name: logo.com | IP: 200.10.100.75 | Version: R3000 Enterprise Filter 2.0.10.3

The NTP Servers window is used for specifying the Network Time Protocol (NTP) servers to be used by the R3000, so that the R3000 is synchronized with computer clocks on the Internet.

Note that the following server IP addresses display in the Servers list box: 128.59.35.142, 142.3.100.15, 129.132.98.11. If necessary, any of these servers can be deleted by selecting the IP address and clicking **Delete**.

NOTE: *If you need to find another NTP server to use, most university Web sites provide these servers for public usage.*

A. In the **NTP Server** field, enter the IP address of the primary NTP server you wish to use for clock settings on your server.

B. Click **Add** to include this IP address in the Servers list box.

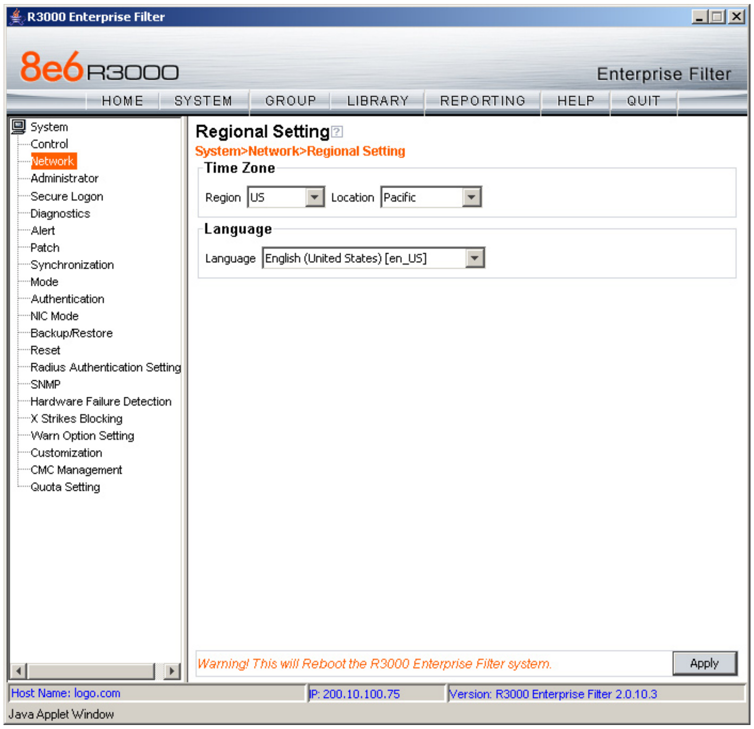
C. Enter two more NTP servers, following the procedures in sub-steps A and B. These will be the secondary and tertiary NTP servers, in order as they appear in the list box.

D. Click **Apply**.

NOTE: *If the primary server fails, the secondary will be used. If the secondary server fails, the tertiary server will be used.*

Network: Regional Setting

From the navigation panel, click Network and choose Regional Setting from the pop-up menu:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
System
Control
Network
Administrator
Secure Logon
Diagnostics
Alert
Patch
Synchronization
Mode
Authentication
NIC Mode
Backup/Restore
Reset
Radius Authentication Setting
SNMP
Hardware Failure Detection
X Strikes Blocking
Warn Option Setting
Customization
CMC Management
Quota Setting
Regional Setting
System>Network>Regional Setting
Time Zone
Language
Apply
Java Applet Window

Region: US

Location: Pacific

Language: English (United States) [en_US]

Warning! This will Reboot the R3000 Enterprise Filter system.

Host Name: logo.com

IP: 200.10.100.75

Version: R3000 Enterprise Filter 2.0.10.3

Make the following selections in the Regional Setting window:

A. At the **Region** pull-down menu, select your country from the available choices.

B. At the **Location** pull-down menu, select the time zone for the specified region.

If necessary, select a language set from the **Language** pull-down menu to display that text in the console.

C. Click **Apply** to apply your settings, and to reboot the R3000.

Physically Connect the R3000IR to the Network

Once your R3000 network parameters are set, you must physically connect the unit to your network. This step requires two standard CAT-5E cables.

***NOTE:** This section requires you to restart the R3000. If you wish to relocate the R3000IR before connecting it to the network, you must first shut down the server instead of restarting it. To shut down the R3000, go to the navigation panel, click Control, and then select ShutDown. Once the server is shut down, you must power on the R3000IR and then log back into the Administrator console.*

A. Restart the server using the steps defined below (i-iii). These steps must always be performed when restarting the R3000IR. ***Never*** reset the server by using the power or reset buttons.

   i. From the navigation panel of the System section of the console, click Control and select Reboot from the pop-up menu to display the Reboot window.
   ii. Click the **Reboot** button.
   iii. From the time you click Reboot, you have approximately 2 minutes to perform sub-steps B through E while the R3000 goes through the reboot process.

B. Disconnect the crossover cable from the R3000IR.

C. Plug one end of a standard CAT-5E cable into the R3000IR’s LAN 1 port.

D. Plug the other end of the CAT-5E cable into an open port on the network hub that handles the Internet traffic you wish to filter.

E. Repeat sub-steps B and C for the R3000IR’s LAN 2 port.

F. Wait until the reboot process has completed, indicated by the drive light staying off for 30 seconds. This process may take 5 to 10 minutes. Proceed to Step 2.

***NOTE:** If you receive a connection failure message during the reboot process, please disregard it, as this often occurs when there is a change in the IP address.*

***NOTE:** To restart the browser window, close both the R3000 Administrator console and the R3000 Introductory Window. Begin a new session by opening a new browser window and then logging back into the Administrator console.*

Step 2: Test the R3000 Console Connection

Now that the R3000IR is physically installed on your network and you have configured its network settings, you need to test the unit to see if it is set up properly.

A. Restore the setup workstation you used for the Network Setup to its original settings, and connect it to the network hub to create a “network workstation.” (You could also use another workstation already on the network that has Internet access.)

B. Launch IE on the network workstation, and enter the IP address you assigned to LAN 1 (Step 1A, Quick Start menu: administration menu, or Step 1B, Network: LAN Settings, sub-step B). Be sure to include the port information **:88** in the address field. For example, if the R3000 were assigned an IP address of 10.10.10.10, you would enter **http://10.10.10.10:88** in the browser window’s address field.

C. Click **Go**. You should be prompted to log into the Administrator console, giving the Username and Password.

If you can access the R3000 Administrator console, the R3000 is functioning on your network and you should proceed to Step 3.

If you cannot access the R3000 Administrator console, please verify the status of the LAN connection in Windows on the network workstation, and then try enabling/disabling the LAN connection. If that fails to work, check the following:

- The R3000IR is turned on.
- The R3000IR is connected to the same hub as your router/firewall.
- Can the PC normally connect to the Internet?
- Is the PC able to ping LAN 1 of the R3000?
- Is the R3000 plugged into a switch instead of a hub?
- Is there a caching server?
- Can the R3000 ping the filtered PC? (Refer to the System Command window in the Diagnostics section of the R3000 User Guide)
- Did you restart the R3000 after changing the network settings?
- Do you have both LAN ports connected to your network hub?
- If still unsuccessful, contact an 8e6 Technologies solutions engineer or technical support representative.

Step 3: Test Filtering or Mobile Client Console Connection

Test Filtering

If this R3000 has been set up in the Invisible, Router, or Firewall mode, once you have accessed the R3000 Administrator console, you should test filtering.

A. Test the R3000's filtering by opening a browser window on a network workstation, and going to **http://test.8e6.net** (an empty site for testing pornography filtering).

B. You should receive a block page. If you do not, contact an 8e6 Technologies solutions engineer or technical support representative.

***NOTE:** Port 22 (SSH) must be open on your network to allow access by remote technical support.*

Test the Mobile Client Console Connection

If this R3000 has been set up in the Mobile mode, you do not need to test filtering. Instead, once you have accessed the R3000 Administrator console, you should verify that the Mobile Client can be accessed by the R3000.

A. Use a workstation on which the Mobile Client is installed that is not on a filtered portion of the LAN. Open a browser window on a network workstation, and then go to **http://test.8e6.net** (an empty site for testing pornography filtering).

B. The connection should be blocked, and the block page served by the R3000 should display in the browser's Address field. If you do not receive a block page, contact an 8e6 Technologies solutions engineer or technical support representative.

***NOTE:** Port 22 (SSH) must be open on your network to allow access by remote technical support.*

Step 4: Set Library Updates

After verifying that the R3000 is correctly installed on your network, you need to activate R3000 library updates. Library updates are critical for filtering as new sites are added to the 8e6 library each day. To activate updates, visit the 8e6 Technologies Web site and enter the activation code that was issued to you by e-mail (also included on the product invoice).

***NOTE:** Port 443 (HTTPS) must be open for outgoing requests so that the R3000 can receive library updates.*

Activate and Register the R3000

Be sure you have a valid host name chosen before activating your account.

A. Open an Internet browser window and go to **http://www.8e6.com/activate**.

B. After reading through the online End User License Agreement, click **Accept** to go to Step 2 of the activation process.

C. Enter your activation code.

D. Click **Submit** to go to the R3000 Activation and Registration page.

E. Verify that your serial number and activation code are the same as shown on this registration page.

F. Fill out the information on this page, including the host name for the public DNS server. ***The entry of the unique host name you've chosen is mandatory in order to receive library updates.***

G. After all information is entered, click **Activate** to activate your service. You should receive confirmation that the R3000 at your host name has been activated.

You may wish to print the confirmation page for future reference in dealing with technical issues.

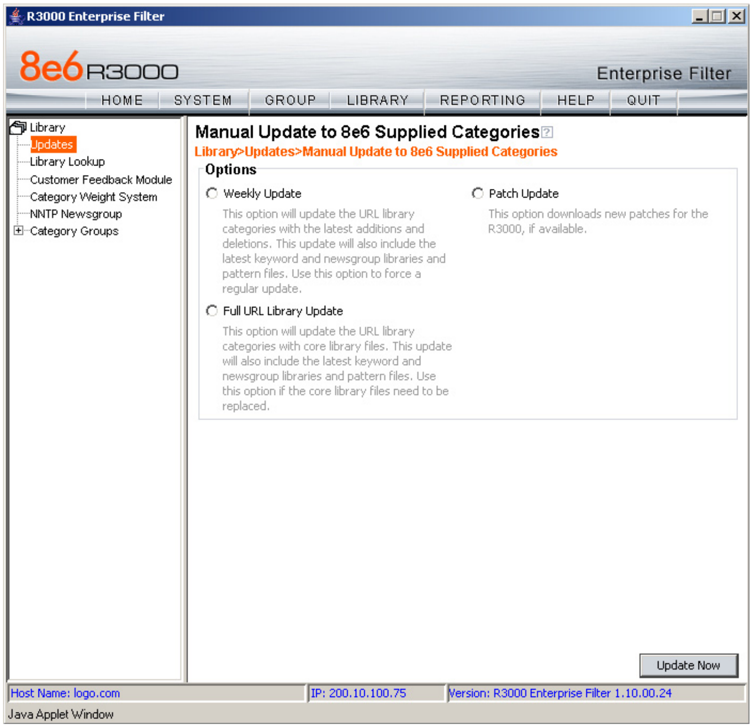
Perform a Complete Library Update

Your R3000IR was shipped with the latest library update for the current software release. However, as new updates continually become available, before you begin using the R3000IR you must perform a complete library update to ensure you have the latest library updates.

To download the latest library updates, go to the R3000 Administrator console.

A. Click the **Library** button at the top of the screen.

B. From the navigation panel, click Updates and select Manual Update from the menu:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
Library
Updates
Library Lookup
Customer Feedback Module
Category Weight System
NNTP Newsgroup
Category Groups
Update Now
Java Applet Window

Manual Update to 8e6 Supplied Categories

Library>Updates>Manual Update to 8e6 Supplied Categories

Options

○ Weekly Update

This option will update the URL library categories with the latest additions and deletions. This update will also include the latest keyword and newsgroup libraries and pattern files. Use this option to force a regular update.

○ Full URL Library Update

This option will update the URL library categories with core library files. This update will also include the latest keyword and newsgroup libraries and pattern files. Use this option if the core library files need to be replaced.

○ Patch Update

This option downloads new patches for the R3000, if available.

Host Name: logo.com | IP: 200.10.100.75 | Version: R3000 Enterprise Filter 1.10.00.24

C. In the Manual Update to 8e6 Supplied Categories window, click the radio button corresponding to **Full URL Library Update**.

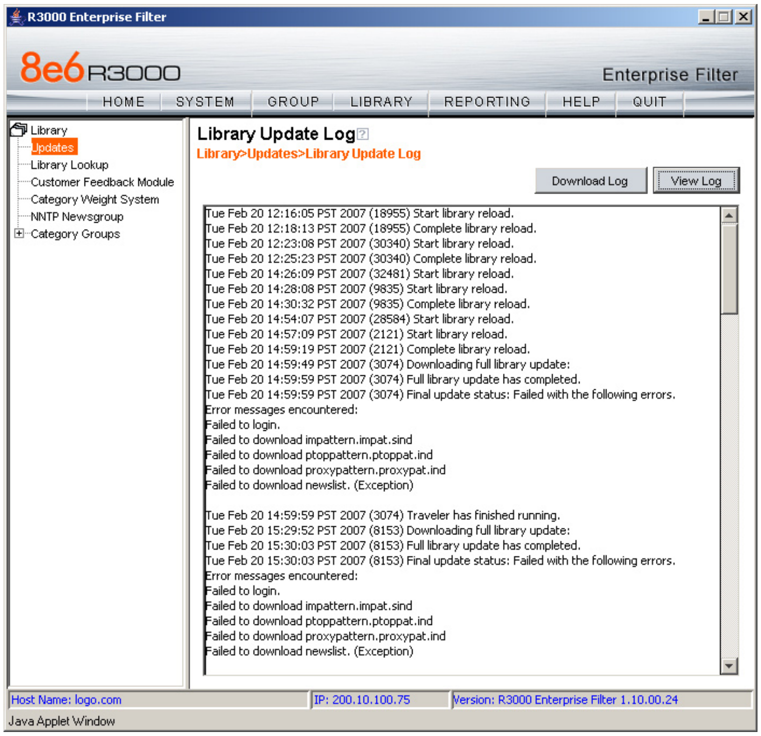
D. Click **Update Now** to begin the update process.

Monitor the Library Update Process

To verify that the library is being updated:

A. From the navigation panel, click Updates and select Library Update Log from the menu.

B. In the Library Update Log window, click **View Log** to display the update activity:


R3000 Enterprise Filter
8e6 R3000
Enterprise Filter
HOME
SYSTEM
GROUP
LIBRARY
REPORTING
HELP
QUIT
Library
Updates
Library Lookup
Customer Feedback Module
Category Weight System
NNTP Newsgroup
Category Groups
Library Update Log
Library>Updates>Library Update Log
Download Log
View Log
Host Name: logo.com
IP: 200.10.100.75
Version: R3000 Enterprise Filter 1.10.00.24
Java Applet Window

```
Tue Feb 20 12:16:05 PST 2007 (18955) Start library reload.
Tue Feb 20 12:18:13 PST 2007 (18955) Complete library reload.
Tue Feb 20 12:23:08 PST 2007 (30340) Start library reload.
Tue Feb 20 12:25:23 PST 2007 (30340) Complete library reload.
Tue Feb 20 14:26:09 PST 2007 (32481) Start library reload.
Tue Feb 20 14:28:08 PST 2007 (9835) Start library reload.
Tue Feb 20 14:30:32 PST 2007 (9835) Complete library reload.
Tue Feb 20 14:54:07 PST 2007 (28584) Start library reload.
Tue Feb 20 14:57:09 PST 2007 (2121) Start library reload.
Tue Feb 20 14:59:19 PST 2007 (2121) Complete library reload.
Tue Feb 20 14:59:49 PST 2007 (3074) Downloading full library update:
Tue Feb 20 14:59:59 PST 2007 (3074) Full library update has completed.
Tue Feb 20 14:59:59 PST 2007 (3074) Final update status: Failed with the following errors.
Error messages encountered:
Failed to login.
Failed to download impattern.impat.sind
Failed to download ptoppattern.ptoppat.ind
Failed to download proxypattern.proxypat.ind
Failed to download newslist. (Exception)

Tue Feb 20 14:59:59 PST 2007 (3074) Traveler has finished running.
Tue Feb 20 15:29:52 PST 2007 (8153) Downloading full library update:
Tue Feb 20 15:30:03 PST 2007 (8153) Full library update has completed.
Tue Feb 20 15:30:03 PST 2007 (8153) Final update status: Failed with the following errors.
Error messages encountered:
Failed to login.
Failed to download impattern.impat.sind
Failed to download ptoppattern.ptoppat.ind
Failed to download proxypattern.proxypat.ind
Failed to download newslist. (Exception)
```

NOTE: *You will be notified in the log when the library has been completely updated by the message: "Full URL Library Update has completed." If this message does not yet display, click* ***View Log*** *again to view the latest information.*

WARNING: *At the conclusion of this step, your R3000 will be actively filtering your network. The R3000 is initially set to filter pornography sites on all of your network traffic associated with the hub to which it is connected.*

Now that the R3000 is filtering your network, the next step is to set up groups and create filtering profiles for group members.

To activate a default filter profile more appropriate for your operations, or to specify a more limited IP range to filter, consult Chapter 2: Group screen in the Global Administrator Section of the R3000 User Guide. Refer to Chapter 1: System screen for information on how to give end users access to acceptable HTTPS sites if strict HTTPS filtering settings are used.

Obtain the latest R3000 User Guide at **http://www.8e6.com/docs/ir_r3000_r2.pdf**.

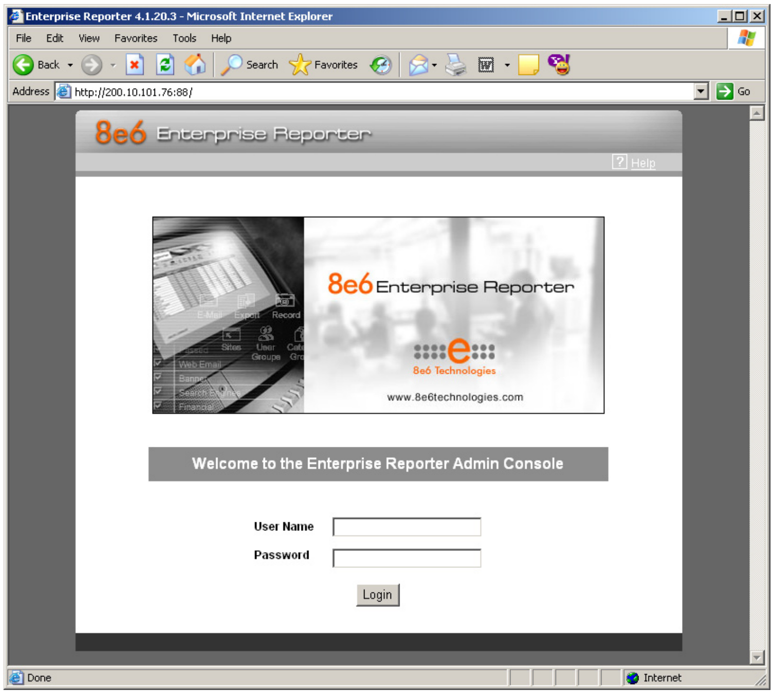
❗ ***IMPORTANT:*** *8e6 recommends reviewing the Best Filtering Practices section to implement setup procedures for the filtering scenarios described within that section.*

Step 5: Change the ER Admin User Name and Password, Set Self-Monitoring

After configuring the R3000, click the **Quit** button at the top of the screen to exit the R3000 Administrator console. You will now need to log in to the ER Administrator console and make some changes to settings in screens.

Log in to the ER Administrator Console

A. In the R3000IR console (see Step 1B: Network Setup, Access the R3000IR Administrator Console), click the link for **Reporting** to open the ER Administrator console:



Enterprise Reporter 4.1.20.3 - Microsoft Internet Explorer

Address http://200.10.101.76:88/

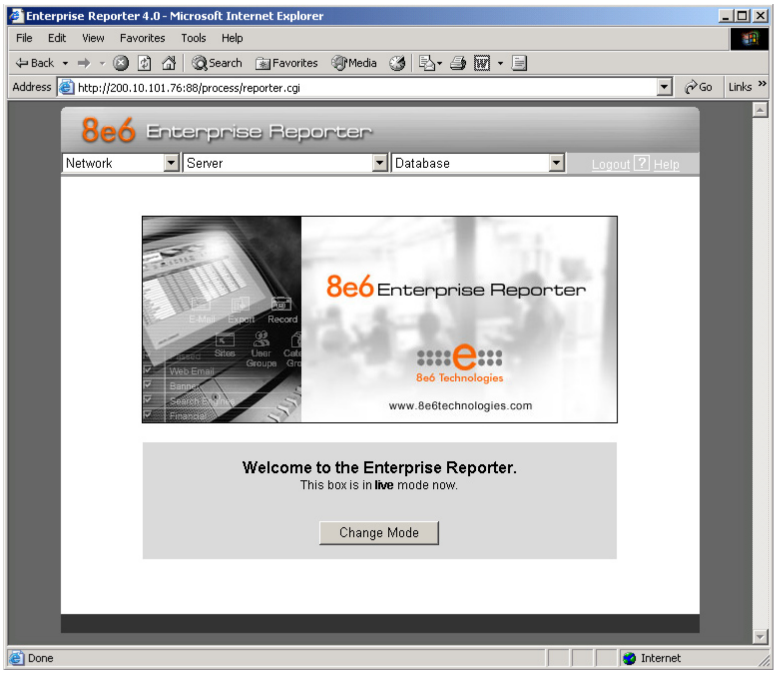
Welcome to the Enterprise Reporter Admin Console

File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Go
8e6 Enterprise Reporter
Help
8e6 Enterprise Reporter
8e6 Technologies
www.8e6technologies.com
User Name
Password
Login
Done
Internet

B. In the **User Name** field, type in ***admin***.

C. In the **Password** field, type in ***reporter***.

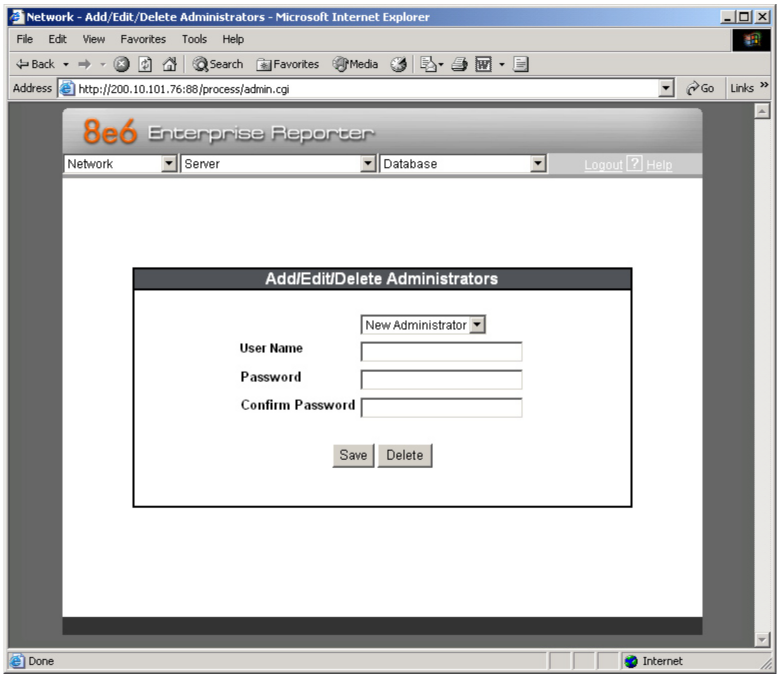
D. Click **OK** to go to the main screen of the ER Administrator console:


Enterprise Reporter 4.0 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.101.76:88/process/reporter.cgi
Go Links
8e6 Enterprise Reporter
Network
Server
Database
Logout ? Help
8e6 Enterprise Reporter
8e6 Technologies
www.8e6technologies.com
Change Mode
Done
Internet

Welcome to the Enterprise Reporter.
This box is in **live** mode now.

Change User Name and Password

A. Set up a new administrator user name and password by clicking on the Network pull-down menu and choosing **Administrators** to display the Add/Edit/Delete Administrators screen:


Network - Add/Edit/Delete Administrators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.101.76:88/process/admin.cgi
Go Links
8e6 Enterprise Reporter
Network
Server
Database
Logout ? Help
Add/Edit/Delete Administrators
New Administrator
User Name
Password
Confirm Password
Save
Delete
Done
Internet

B. Select **New Administrators** from the pull-down menu.

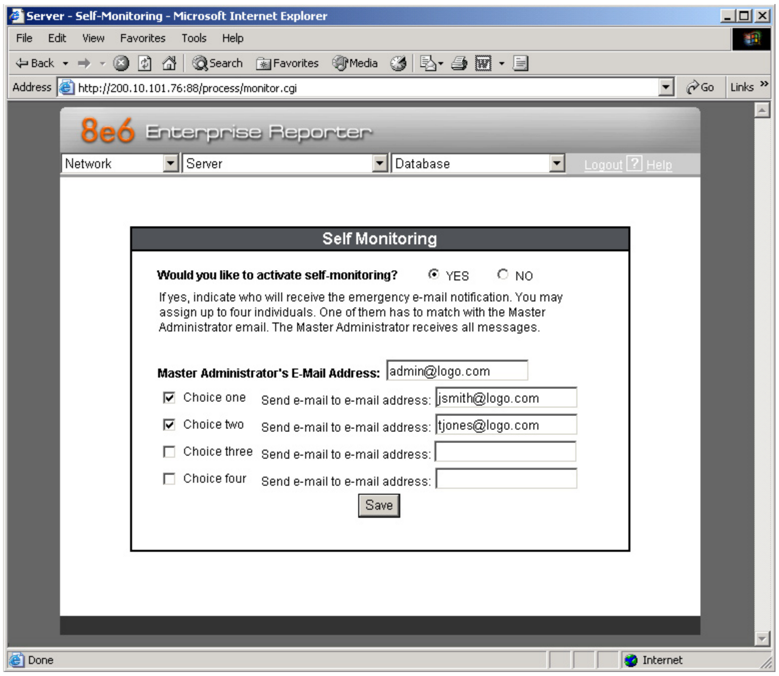
C. Enter a **User Name** and **Password**.

D. In the **Confirm Password** field, re-enter the password.

E. Click **Save**.

Set Self-Monitoring

A. From the Server pull-down menu, choose **Self-Monitoring** to display the Self Monitoring screen:


Server - Self-Monitoring - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.101.76:88/process/monitor.cgi
Go Links
8e6 Enterprise Reporter
Network
Server
Database
Logout
Help
Done
Internet

Self Monitoring

Would you like to activate self-monitoring? ● YES ○ NO

If yes, indicate who will receive the emergency e-mail notification. You may assign up to four individuals. One of them has to match with the Master Administrator email. The Master Administrator receives all messages.

Master Administrator's E-Mail Address: admin@logo.com

☑ Choice one Send e-mail to e-mail address: jsmith@logo.com

☑ Choice two Send e-mail to e-mail address: tjones@logo.com

☐ Choice three Send e-mail to e-mail address:

☐ Choice four Send e-mail to e-mail address:

Save

B. Choose **YES** to activate monitoring.

C. Enter the **Master Administrator’s E-Mail Address**.

D. Click **Choice one** and enter an e-mail address of an individual in your organization that you would like notified if the ER detects any problems when processing data. This can be the same e-mail address entered in the previous field. Enter up to four e-mail addresses.

E. Click **Save**.

Now that the ER server settings have been made, you need to configure a client workstation for reporting.

Step 6: Client Workstation Configuration

Once your ER is installed, you need to be sure the workstation that will run the client has the following minimum requirements:

- Pentium III class processor or greater
- 512 MB RAM minimum, 1 GB RAM recommended
- 1,024 x 768 display
- 2 GB free hard drive space
- Windows 2000 or XP, or Macintosh OS X operating system
- Internet Explorer Version 6.0 or later, Firefox 1.5, or Safari 2.0 Web browser
- Pop-up blocking software disabled, if installed
- High-speed connection to ER server

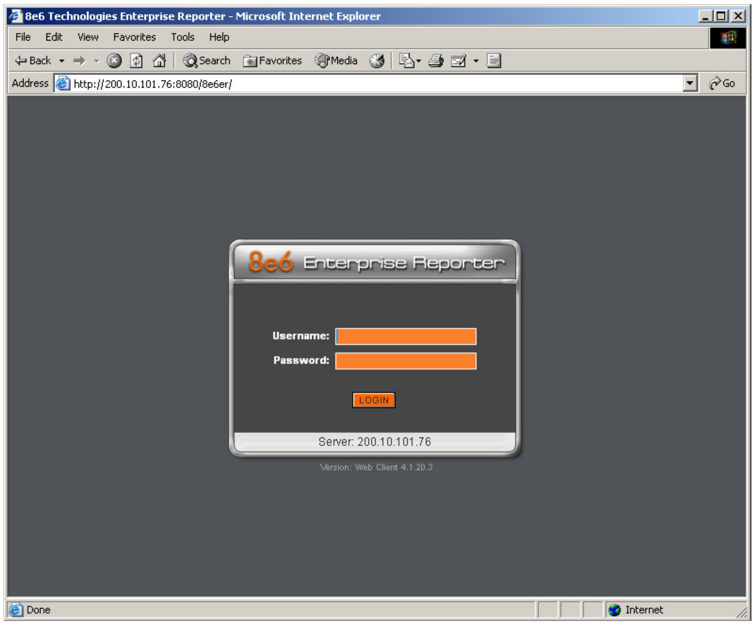
Go to the ER server and apply the latest software to the server, following the procedures documented in the Software Update screen sub-section of the ER Administrator User Guide. The CD-ROM supplied with the ER contains the ER Administrator User Guide, the latest version which can be downloaded from our Web site at: **http://www.8e6.com/docs/ir_er4server.pdf**.

NOTE: *The ER Web Client User Guide is on the CD-ROM, the latest version which can be downloaded from our Web site at **http://www.8e6.com/docs/er4_wclient.pdf**.*

Step 7: Launch the ER Client

A. Launch IE, enter **http://x.x.x.x:8080** or **https://x.x.x.x:8443** in the address window (in which “x.x.x.x” represents the IP address of the ER server), and then click **Go** to access the login window of the ER client.

B. Enter your **Username** and **Password**, and then click **LOGIN** to access the main screen of the client:


8e6 Technologies Enterprise Reporter - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go
8e6 Enterprise Reporter
Username:
Password:
LOGIN
Done
Internet

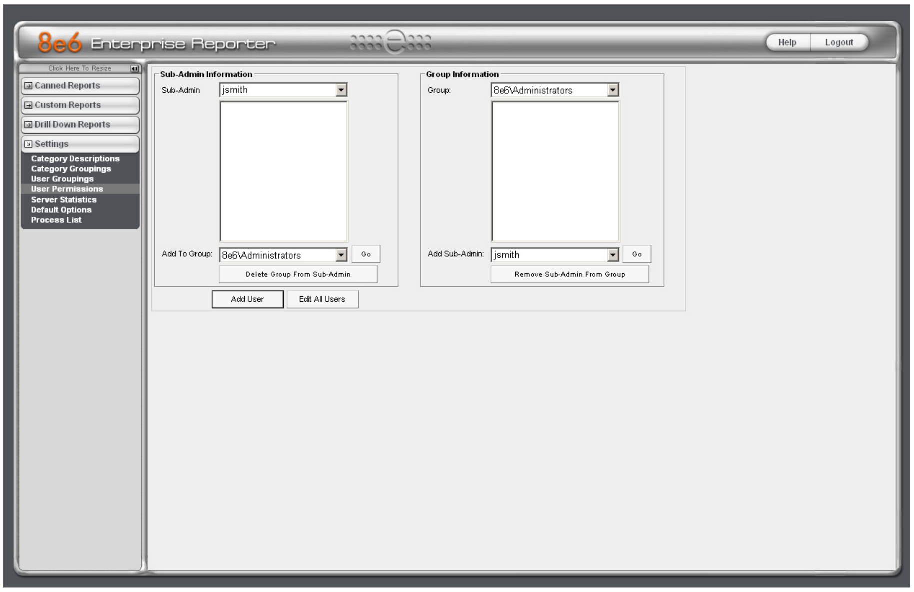
Address http://200.10.101.76:8080/8e6er/

Server: 200.10.101.76

Version: Web Client 4.1.20.3

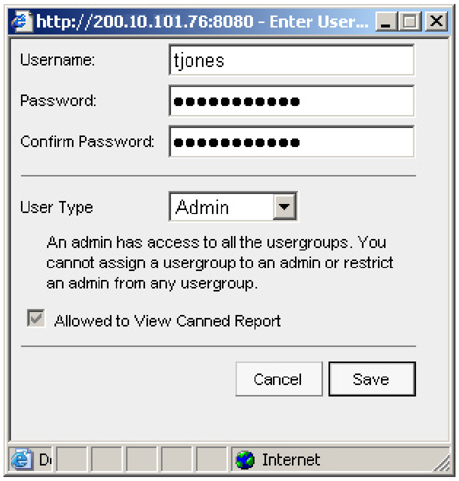
NOTE: *If you do not have your own Username and Password set up in the ER client, the default Username is **manager** and the default Password is **8e6ReporT**.*

C. In the navigation panel, select **Settings**, and then choose **User Permissions** from the menu:


8e6 Enterprise Reporter
Help
Logout
Click Here To Resize
Canned Reports
Custom Reports
Drill Down Reports
Settings
Category Descriptions
Category Groupings
User Groupings
User Permissions
Server Statistics
Default Options
Process List
Sub-Admin Information
Group Information
Go
Delete Group From Sub-Admin
Remove Sub-Admin From Group
Add User
Edit All Users

Sub-Admin: jsmith
Add To Group: 8e6\Administrators
Group: 8e6\Administrators
Add Sub-Admin: jsmith

D. Click **Add User** to open the Enter User Permissions dialog box:


http://200.10.101.76:8080 - Enter User...
Cancel
Save
D
Internet

Username: tjones
Password: ●●●●●●●●●●●●
Confirm Password: ●●●●●●●●●●●●
User Type: Admin

An admin has access to all the usergroups. You cannot assign a usergroup to an admin or restrict an admin from any usergroup.

☑ Allowed to View Canned Report

E. Enter the **Username**.

F. Enter the **Password**, and **Confirm Password**.

G. Select the **User Type** ("Admin" or "Sub-Admin").

H. Click **Save** to close the dialog box, and to add the username to the user list.

I. Exit the client. You can now launch the client and enter the password you just set up.

NOTE: *For instructions on logging into the client after initial set up, refer to the ER Web Client User Guide.*

CONCLUSION

Congratulations; you have completed the R3000IR quick start procedures. Now that the R3000 and ER are set up on your network, once the ER database is populated with logs from the R3000, the client can be used for generating reports.

Initially, you will only be able to report on IP addresses. To implement user names in ER reporting, please consult the ER Administrator User Guide.

Refer to the ER Web Client User Guide for information on generating reports.

NOTE: *If you cannot view reports, or if your specific environment is not covered in the ER Administrator User Guide, contact an 8e6 Technologies solutions engineer or technical support representative. Port 22 (SSH) and Port 3306 (SQL) must be open on your network to allow access by remote technical support.*

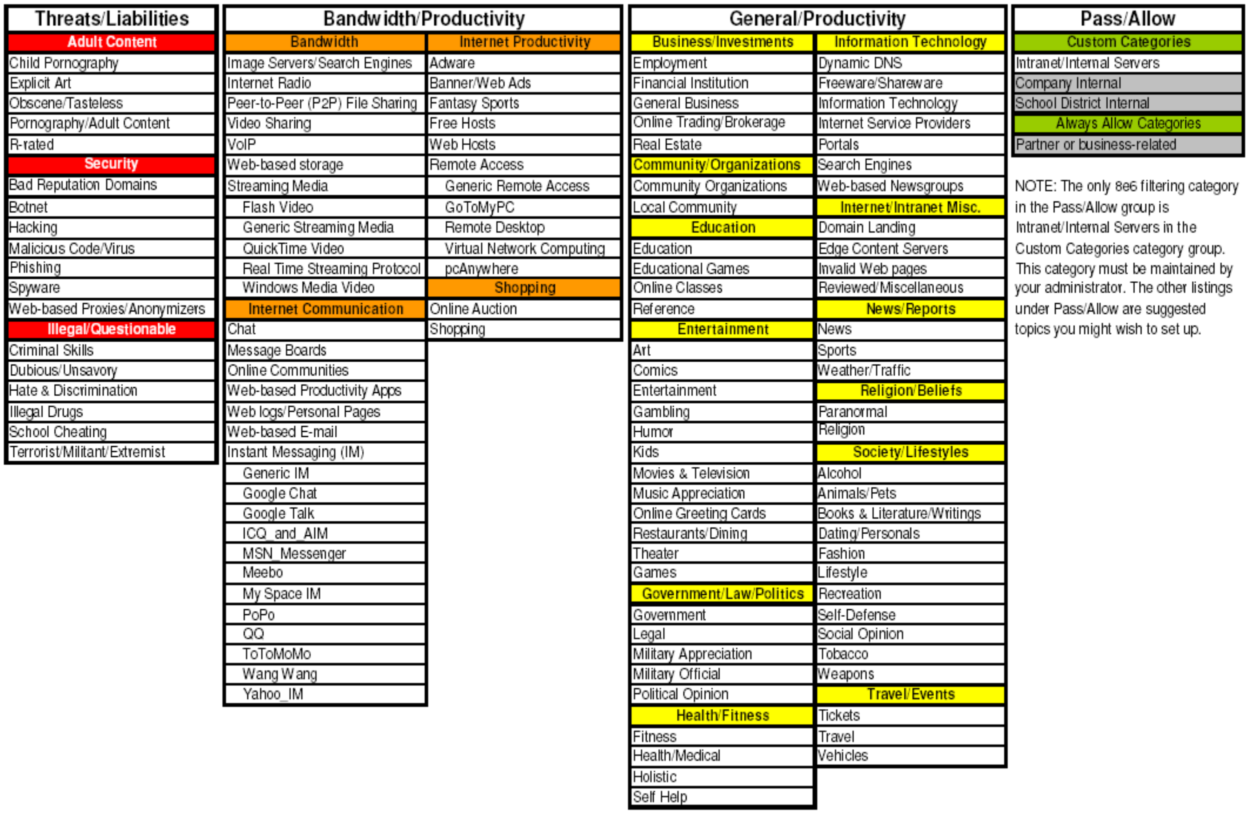
BEST FILTERING PRACTICES

Threat Class Groups

8e6's filtering library currently consists of 103 library filtering categories, each placed in one of the 20 filtering category groups defined in the interface: Adult Content, Bandwidth, Business/Investments, Community/Organizations, Education, Entertainment, Government/Law/Politics, Health/Fitness, Illegal/Questionable, Information Technology, Internet Communication, Internet Productivity, Internet/Intranet Misc., News/Reports, Religion/Beliefs, Security, Shopping, Society/Lifestyles, Travel/Events, and Custom Categories.

Outside of the interface, we have also grouped these library categories into four Threat Class Groups, based on the type of security level that best defines them:

- Threats/Liabilities
- Bandwidth/Productivity
- General/Productivity
- Pass/Allow



Threats/Liabilities	Bandwidth/Productivity		General/Productivity		Pass/Allow
Adult Content	**Bandwidth**	**Internet Productivity**	**Business/Investments**	**Information Technology**	**Custom Categories**
Child Pornography	Image Servers/Search Engines	Adware	Employment	Dynamic DNS	Intranet/Internal Servers
Explicit Art	Internet Radio	Banner/Web Ads	Financial Institution	Freeware/Shareware	Company Internal
Obscene/Tasteless	Peer-to-Peer (P2P) File Sharing	Fantasy Sports	General Business	Information Technology	School District Internal
Pornography/Adult Content	Video Sharing	Free Hosts	Online Trading/Brokerage	Internet Service Providers	**Always Allow Categories**
R-rated	VoIP	Web Hosts	Real Estate	Portals	Partner or business-related
Security	Web-based storage	Remote Access	**Community/Organizations**	Search Engines	
Bad Reputation Domains	Streaming Media	Generic Remote Access	Community Organizations	Web-based Newsgroups	
Botnet	Flash Video	GoToMyPC	Local Community	**Internet/Intranet Misc.**	
Hacking	Generic Streaming Media	Remote Desktop	**Education**	Domain Landing	
Malicious Code/Virus	QuickTime Video	Virtual Network Computing	Education	Edge Content Servers	
Phishing	Real Time Streaming Protocol	pcAnywhere	Educational Games	Invalid Web pages	
Spyware	Windows Media Video	**Shopping**	Online Classes	Reviewed/Miscellaneous	
Web-based Proxies/Anonymizers	**Internet Communication**	Online Auction	Reference	**News/Reports**	
Illegal/Questionable	Chat	Shopping	**Entertainment**	News	
Criminal Skills	Message Boards		Art	Sports	
Dubious/Unsavory	Online Communities		Comics	Weather/Traffic	
Hate & Discrimination	Web-based Productivity Apps		Entertainment	**Religion/Beliefs**	
Illegal Drugs	Web logs/Personal Pages		Gambling	Paranormal	
School Cheating	Web-based E-mail		Humor	Religion	
Terrorist/Militant/Extremist	Instant Messaging (IM)		Kids	**Society/Lifestyles**	
	Generic IM		Movies & Television	Alcohol	
	Google Chat		Music Appreciation	Animals/Pets	
	Google Talk		Online Greeting Cards	Books & Literature/Writings	
	ICQ_and_AIM		Restaurants/Dining	Dating/Personals	
	MSN_Messenger		Theater	Fashion	
	Meebo		Games	Lifestyle	
	My Space IM		**Government/Law/Politics**	Recreation	
	PoPo		Government	Self-Defense	
	QQ		Legal	Social Opinion	
	ToToMoMo		Military Appreciation	Tobacco	
	Wang Wang		Military Official	Weapons	
	Yahoo_IM		Political Opinion	**Travel/Events**	
			Health/Fitness	Tickets	
			Fitness	Travel	
			Health/Medical	Vehicles	
			Holistic		
			Self Help		

NOTE: The only 8e6 filtering category in the Pass/Allow group is Intranet/Internal Servers in the Custom Categories category group. This category must be maintained by your administrator. The other listings under Pass/Allow are suggested topics you might wish to set up.

Please review the Filtering Scenarios sub-section for information on configuring the R3000 to fulfill the filtering scenarios assigned to each of the four Threat Class Groups.

Filtering Scenarios

This collection of filtering scenarios is designed to help you get started filtering the network. Each scenario is followed by R3000 setup information. Please consult the “How to” section in the index of the R3000 User Guide for pages containing detailed, step-by-step instructions on configuring and/or using the tools and features in that scenario.

I. Threats/Liabilities

1. Category block

Block categories that threaten your network/organization. In pertinent profiles, block access to the Security category group and other categories containing content that threaten your organization.

To block categories in a profile, go to:

- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: use library categories in a profile

2. Rule block

Use a rule to block categories that threaten your network/organization. Create a rule that blocks access to the Security category group and other categories containing content that threaten your organization, and then apply this rule to pertinent profiles. Or use a defined rule—such as the 8e6 CIPA Compliance rule, if in the educational sector—to block related categories.

To create a rule and block categories in a profile, go to:

- GROUP: Group > Global Group > Rules
- Group > IP > member > member profile > Category tab
  or Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: use rules
• How to: use library categories in a profile

3. X-Strike on blocked categories

Lock out users from workstations after “X” number of attempts are made to access content that could endanger your network/organization. Enable and configure the X Strikes Blocking feature, specifying categories that threaten your organization. Enable the X Strikes Blocking filter option in applicable profiles. The user receives a block page and is locked out of Internet/Intranet access after the specified number of “strikes” are made to any of these categories.

To block categories in a profile using the X Strikes Blocking feature, go to:

- SYSTEM: System > X Strikes Blocking > Configuration tab, and Categories tab
- GROUP: Group > IP > member > member Profile > Filter Options tab, X Strikes Blocking enabled
  or GROUP: Group > Global Group > Global Group Profile > Filter Options tab (X Strikes Blocking enabled)

In the R3000 User Guide index, see:
• How to: set up X Strikes Blocking
• How to: set up profile options

4. Custom Lock, Block, Warn, X Strikes, Quota pages

Customize a lock, block, warning, X Strikes, or quota page. Modify page contents to point to a URL within your organization, send a request to your administrator's email address, or include verbiage of your choice that informs users of their Internet usage activities that triggered the page.

To customize pages, go to:

- SYSTEM: System > Customization > Common Customization window, and other applicable customization windows

In the R3000 User Guide index, see:
• How to: customize pages

5. URL Keywords

Block access to network-endangering content via URL keywords. In pertinent library categories, enter URL keywords to be blocked. Block these categories in applicable profiles.

To set up URL keywords to be blocked, go to:

- LIBRARY: Library > Category Groups > category > URL Keywords
- GROUP: Group > IP > member > member Profile > Filter Options tab (URL Keyword Filter Control enabled)
  or GROUP: Group > Global Group > Global Group Profile > Filter Options tab (URL Keyword Filter Control enabled)

In the R3000 User Guide index, see:
• How to: set up URL Keywords
• How to: set up profile options

6. Search Engine Keywords

Block access to network-endangering content via search engine keywords. In pertinent library categories, enter SE keywords to be blocked. Block these categories in applicable profiles.

To set up Search Engine Keywords to be blocked, go to:
- LIBRARY: Library > Category Groups > category > Search Engine Keywords
- GROUP: Group > IP > member > member Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)
  or GROUP: Group > Global Group > Global Group Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)

In the R3000 User Guide index, see:
• How to: set up Search Engine Keywords
• How to: set up profile options

7. Custom Category (blocked)

Add a category to block content that could endanger your network/organization. Create a custom category with contents tailored to safeguard your organization. Block this category in appropriate profiles.

To set up a custom category and block it, go to:
- LIBRARY: Library > Category Groups > Custom Categories > Add Category
- GROUP: Group > IP > member > member Profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: set up a custom category
• How to: use library categories in a profile

8. Minimum Filtering Level

At the root level, block categories that could endanger your network/organization. Configure the Minimum Filtering Level to block specified categories, and do the same in the Global Group Profile.

To configure the minimum filtering level, go to:
- GROUP: Group > Global Group > Minimum Filtering Level
- Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: configure the Minimum Filtering Level
• How to: use library categories in a profile: Global Group Profile

9. Override Account bypass

Use an Override Account to grant a user access to categories blocked at the root level. To grant designated users access to globally-blocked categories, set up an Override Account at the Global Group level, or enable the option to allow the Minimum Filtering Level to be bypassed with an Override Account, and then set up the Override Account at the group level.

To set up an override account at the Global Group level, go to:
- GROUP: Group > Global Group > Override Account window

To configure the bypass feature and set up a group level override account, go to:
- GROUP: Group > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Group > IP > group > Override Account window

In the R3000 User Guide index, see:
• How to: set up an Override Account: Global Group
or:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up an Override Account: Group profile

---

10. Exception URL bypass

Use exception URLs to grant users access to URLs blocked at the root. To grant users access to globally-blocked URLs, enable the exception URL bypass option in the Minimum Filtering Level. For these users, add the exception URLs in their profiles.

To set up the Exception URL bypass feature and let users bypass blocked URLs, go to:
- GROUP: Group > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Group > IP > member > Exception URL window

In the R3000 User Guide index, see:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up Exception URLs

---

11. Proxy Patterns

Prevent users from using proxy patterns to bypass the Internet filter. Enable Pattern Blocking for all users. In the profile, block Security > Web-based Proxies/Anonymizers.

To set up the proxy pattern blocking feature and apply it to profiles, go to:
- SYSTEM: System > Control > Filter window
- GROUP: Group > IP > member > member Profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
- *How to: configure filtering*
- *How to: use library categories in a profile*

12. File type blocking

Prevent users from downloading and using executable files that may threaten your network security. Create a custom category for file extensions and add ".exe" to the URL Keyword list. Other files you might include in the list are: .dll, .ocx, .scr, .bat, .pif, .cpl, .cmd, .hta, .lnk, .inf, .sys, .vbs, .vb, .wsc, .wsh, .wsf. Do NOT include ".com" in the list, or the files will not be found and blocked. In the applicable profiles, block this custom category and enable both URL Keyword Filter Control and extension options.

To set up file type blocking and apply this feature to profiles, go to:
- LIBRARY: Library > Category Groups > Custom Categories > Add Category
- Library > Custom Categories > category > URL Keywords
- GROUP: Group > IP > member > member Profile > Category tab, and Filter Options tab (URL Keyword Filter Control and extension options enabled) or GROUP: Group > Global Group > Global Group Profile > Category tab, and Filter Options tab (URL Keyword Filter Control and extension options enabled)

In the R3000 User Guide index, see:
- *How to: set up a custom category*
- *How to: set up URL Keywords: Custom Categories*
- *How to: use library categories in a profile*
- *How to: set up profile options*

II. Bandwidth/Productivity

1. Time Quota/Hit Quota

Limit time spent in PASSED categories to prevent excessive bandwidth usage and increase productivity. Enable the Quota Settings feature, and configure the Seconds Per Hit. Set up pertinent categories in the user's profile with quotas so the user is notified and then locked out of those categories after all minutes in the quota have been used.

To set up the quota feature and configure profiles to use this feature, go to:
- SYSTEM: System > Quota Setting window
- GROUP: Group > IP > member profile > Category tab (Quota column) or Group > Global Group > Global Group Profile > Category tab (Quota column)

In the R3000 User Guide index, see:
- *How to: set up Quotas*
- *How to: use library categories in a profile*

2. Overall Quota

Restrict all quota time in a profile to improve bandwidth usage and productivity. Cap the amount of time a user spends in all quota-marked categories by enabling the Overall Quota option and specifying the number of minutes the end user can visit quota-marked categories before being notified and then locked out of these categories.

To set up the quota feature and configure profiles to use the Overall Quota feature, go to:
- SYSTEM: System > Quota Setting window
- GROUP: Group > IP > member profile > Category tab (Overall Quota)
  or Group > Global Group > Global Group Profile > Category tab (Overall Quota)

In the R3000 User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

3. Time Based Profiles

Schedule a profile to be used at a specific time. Set up one or more profiles for each user or group to be active at a scheduled time.

To set up Time Profiles, go to:
- GROUP: Group > IP > member > Time Profile window

In the R3000 User Guide index, see:
• How to: set up a Time Profile

4. Warn option with low filter settings

Warn users before they access unacceptable content that their Internet activities are logged. Set HTTPS filtering at the “low” level, and then configure the number of minutes for the interval the warning page will re-display for any user who attempts to access content deemed unacceptable. In the end user’s profile, set the Warn categories.

To set up and use the warn option, go to:
- SYSTEM: System > Control > Filter window
- System > Warn Option Setting window
- GROUP: Group > IP > member > member profile > Category tab (Warn column)
  or GROUP: Group > Global Group > Global Group Profile > Category tab (Warn column)

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: configure the Warn Option Setting
• How to: use library categories in a profile

5. Warn-strike

Warn users before they access unacceptable content and may be locked out of the Internet. Enable the Warn feature along with X Strikes Blocking. After the end user is warned for the designated number of times defined in X Strikes Blocking, that user is locked out of all Internet/intranet access.

To set up and use the warn option with X Strikes Blocking, go to:
- SYSTEM: System > X Strikes Blocking window
- System > Warn Option Setting window
- GROUP: Group > IP > member > member profile > Category Profile tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)
  or GROUP: Group > Global Group > Global Group Profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)

In the R3000 User Guide index, see:
• How to: set up X Strikes Blocking
• How to: configure the Warn Option Setting
• How to: use library categories in a profile
• How to: set up profile options

6. P2P patterns

Block P2P services. Enable Pattern Blocking for all users. In the profile, block Bandwidth > Peer-to-peer/File Sharing category.

To block P2P services, go to:
- SYSTEM: System > Control > Filter window
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

7. IM patterns

Block IM services. Enable Pattern Blocking for all users. In the profile, block Internet Communication > Chat and Instant Messaging (IM) categories.

To block IM services, go to:
- SYSTEM: System > Control > Filter window
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

8. Game patterns

Block game patterns. Enable Pattern Blocking for all users. In the profile, block Entertainment > Games category.

To block game patterns, go to:
- SYSTEM: System > Control > Filter window
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

9. Streaming Media patterns

Block streaming media patterns. Enable Pattern Blocking for all users. In the profile, block Bandwidth > Streaming Media category.

To block streaming media patterns, go to:
- SYSTEM: System > Control > Filter window
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

10. Remote Access patterns

Block remote access patterns. Enable Pattern Blocking for all users. In the profile, block Internet Productivity > Remote Access category.

To block remote access patterns, go to:
- SYSTEM: System > Control > Filter window
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

---

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

11. HTTPS settings

Establish the security level for HTTPS site access. Configure HTTPS filter settings in the Filter window. Choose “None” if you do not want the R3000 to filter HTTPS sites, “Low” if you want the R3000 to filter HTTPS sites without having the R3000 communicate with IP addresses or hostnames of HTTPS servers, “Medium” if you want the R3000 to communicate with HTTPS servers in order to get the URL from the certificate for URL validation only (this is the default setting), or “High” if you want the R3000 to communicate with HTTPS servers to obtain the certificate with a very strict validation of the return URL.

To configure HTTPS settings, go to:
- SYSTEM: System > Control > Filter window

In the R3000 User Guide index, see:
• How to: configure filtering

12. Category block

Block the Bandwidth category. Set the Bandwidth category to be blocked in pertinent profiles.

To block the Bandwidth category, go to:
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: use library categories in a profile

13. Rule block

Use a rule to block the Bandwidth category. Create a rule that blocks the Bandwidth category and apply this rule to pertinent profiles.

To create and block a rule for the Bandwidth category, go to:

- GROUP: Group > Global Group > Rules
- Group > IP > member > member profile > Category tab
  or Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: use rules
• How to: use library categories in a profile

14. SE Keywords

Block specific search engine keywords to restrict access to bandwidth-consumptive categories. In pertinent library categories, enter URL keywords to be blocked. Block these categories in the profile.

To set up search engine keywords and block them in a profile, go to:

- LIBRARY: Library > Category Groups > category group > category > Search Engine Keywords
- GROUP: Group > IP > member > member Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)
  or GROUP: Group > Global Group > Global Group Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)

In the R3000 User Guide index, see:
• How to: set up Search Engine Keywords
• How to: set up profile options

15. URL Keywords

Block specific URL keywords to restrict access to bandwidth-consumptive categories. In pertinent library categories, enter SE keywords to be blocked. Block these categories in the profile.

To set up and block URL keywords in a profile, go to:

- LIBRARY: Library > Category Groups > category group > category > URL Keywords
- GROUP: Group > IP > member > member Profile > Filter Options tab (URL Keyword Filter Control enabled)
  or GROUP: Group > Global Group > Global Group Profile > Filter Options tab (URL Keyword Filter Control enabled)

In the R3000 User Guide index, see:
• How to: set up URL Keywords
• How to: set up profile options

16. Custom Block/Warn/X Strikes/Quota pages

Customize a block, warning, X Strikes, or quota pages. Modify page contents to point to a URL within your organization, send a request to your administrator's email address, or include verbiage of your choice that informs users of their Internet usage activities that triggered the page.

To customize pages, go to:

- SYSTEM: System > Customization > Common Customization window, and other applicable customization windows

In the R3000 User Guide index, see:
• How to: customize pages

17. Real Time Probe information

Monitor Internet usage activity in real time. Enable Real Time Probe reporting. Create a probe to monitor Internet traffic by category, user IP address, username, or URL. Set up a schedule for the probe to run during a specific time period.

To enable and use Real Time Probe reporting, go to:

- REPORTING: Report > Real Time Probe > Configuration tab
- Real Time Probe > Go to Real Time Probe Reports GUI link > Real Time Probe Reports > Create tab

In the R3000 User Guide index, see:
• How to: set up Real Time Probes

III. General/Productivity

1. Warn Feature with higher thresholds

Warn users before they access unacceptable content. Set HTTPS filtering at the "high" level to block certificates that may be questionable. Configure Warning settings. In the end user's profile, apply the warn option to pertinent categories. The end user may not be able to access all requested sites due to high settings, and will receive the warning message for excessive Internet usage.

To set up and use the warn option with high filter settings, go to:
- SYSTEM: System > Control > Filter window
- System > Warn Option Setting window
- GROUP: Group > IP > member profile > Category tab (Warn column)
  or GROUP: Group > Global Group > Global Group Profile > Category tab (Warn column)

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: configure the Warn Option Setting
• How to: use library categories in a profile

---

2. Warn-strike with higher thresholds

Warn users before they access unacceptable content and may be locked out of the Internet. Set HTTPS filtering at the "high" level, configure Warning settings, and enable X Strikes Blocking. In the end user's profile, set the Warn categories, and enable X Strikes Blocking. The end user may not be able to access all requested sites due to high settings, and will receive the warning message for excessive Internet usage. After being warned for the designated number of times defined in X Strikes Blocking, that user is locked out of all Internet/Intranet access.

To set up and use the warn option, go to:
- SYSTEM: System > Control > Filter window
- System > X Strikes Blocking window
- System > Warn Option Setting window
- GROUP: Group > IP > member > member profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)
  or GROUP: Group > Global Group > Global Group Profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)

In the R3000 User Guide index, see:
• How to: configure filtering
• How to: set up X Strikes Blocking
• How to: configure the Warn Option Setting
• How to: use library categories in a profile
• How to: set up profile options

---

3. Time Quota/Hit Quota

Limit time spent in PASSED categories to increase productivity. Enable the Quota Settings feature, and configure the Seconds Per Hit. Set up pertinent categories in the user's profile with quotas so the user is notified and then locked out of those categories after all minutes in the quota have been used.

To set up the Quota feature and use quotas in profiles, go to:

- SYSTEM: System > Quota Setting window
- GROUP: Group > IP > member > profile > Category tab (Quota column) or GROUP: Group > Global Group > Global Group Profile > Category tab (Quota column)

In the R3000 User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

---

4. Time Based Profiles

Schedule a profile to be used at a specific time. Set up one or more profiles for each user or group to be active at a scheduled time.

To set up and use time profiles, go to:

- GROUP: Group > IP > member > Time Profile window

In the R3000 User Guide index, see:
• How to: set up a Time Profile

---

5. Overall Quota

Restrict all quota time in a profile to improve productivity. Cap the amount of time a user spends in all quota-marked categories by enabling the Overall Quota option and specifying the number of minutes the end user can visit quota-marked categories before being notified and then locked out of these categories.

To set up the quota feature and configure profiles to use the Overall Quota feature, go to:

- SYSTEM: System > Quota Setting window
- GROUP: Group > IP > member profile > Category tab (Overall Quota) or Group > Global Group > Global Group Profile > Category tab (Overall Quota)

In the R3000 User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

---

6. Customize an 8e6 Supplied Category

Include region-specific content in an 8e6 Supplied category. Add/delete content to/from an existing 8e6 Supplied Category that only includes content pertinent to your organization or region that should be blocked. Apply this category to a profile.

To customize and use an 8e6 Supplied Category in a profile, go to:

- LIBRARY: Library > Category Groups > category group > category (add/delete URLs, URL Keywords, Search Engine Keywords)
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

---

In the R3000 User Guide index, see:
• How to: set up URLs in categories: 8e6 Supplied Categories
• How to: use library categories in a profile

---

7. Local category adds/deletes

Include region-specific content in a Custom category. Set up a custom category that only includes content pertinent to your organization or region that should be blocked. Apply this category to a profile.

To create a Custom Category and use it in a profile, go to:

- LIBRARY: Library > Category Groups > Custom Categories > Add Category (add URLs, URL Keywords, Search Engine Keywords)
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

---

In the R3000 User Guide index, see:
• How to: set up a custom category
• How to: use library categories in a profile

---

8. Custom Block/Warn/X Strikes/Quota pages

Customize a block, warning, X Strikes, or quota pages. Modify page contents to point to a URL within your organization, send a request to your administrator's email address, or include verbiage of your choice that informs users of their Internet usage activities that triggered the page.

To customize pages, go to:

- SYSTEM: System > Customization > Common Customization window, and other applicable customization windows

---

In the R3000 User Guide index, see:
• How to: customize pages

IV. Pass/Allow

1. Always Allow Custom Category

Create a white list custom category. Set up an Always Allow category and add all URLs deemed acceptable. Apply this category to all pertinent profiles.

To create a white list custom category and use it in a profile, go to:

- LIBRARY: Library > Category Groups > Custom Categories > Add Category (add URLs, URL Keywords, Search Engine Keywords)
- GROUP: Group > IP > member > member profile > Category tab
  or GROUP: Group > Global Group > Global Group Profile > Category tab

In the R3000 User Guide index, see:
• How to: set up a custom category
• How to: use library categories in a profile

2. URL exceptions

Use Exception URLs to let specified individuals bypass the Minimum Filtering Level. Enable the option to bypass the Minimum Filtering Level using exception URLs. Enter the exception URLs in the applicable profile.

To set up the Exception URL bypass feature and let users bypass blocked URLs, go to:

- GROUP: Group > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Group > IP > member > Exception URL window

In the R3000 User Guide index, see:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up Exception URLs

3. IP exceptions

Use Exception URLs to grant individuals access to IPs blocked by the Minimum Filtering Level. Enable the option to bypass the Minimum Filtering Level using exception URLs. Enter the exception Internet/intranet IP addresses in the applicable profile.

To set up the Exception URL bypass feature and let users bypass blocked IP addresses, go to:

- GROUP: Group > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Group > IP > member > Exception URL window

In the R3000 User Guide index, see:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up Exception URLs

4. Override Accounts

Set up override accounts to grant specified users access to URLs blocked for general users. Enable the option to bypass the Minimum Filtering Level using an override account. Create the override account profile, including the accessible categories. To grant designated users access to globally-blocked categories, set up an Override Account at the Global Group level, or enable the option to allow the Minimum Filtering Level to be bypassed with an Override Account, and then set up the Override Account at the member level.

To set up an override account at the Global Group level, go to:
- GROUP: Group > Global Group > Override Account window

To configure the bypass feature and set up a group level override account, go to:
- GROUP: Group > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Group > IP > group > Override Account window

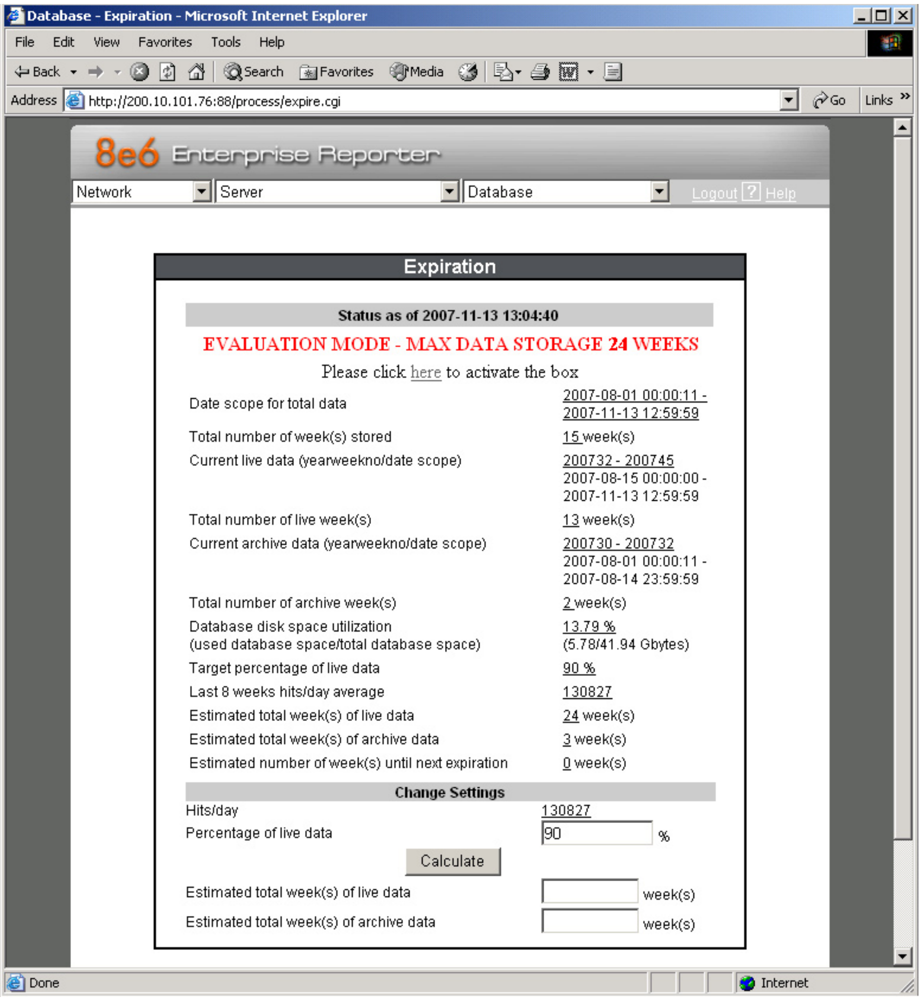
In the R3000 User Guide index, see:
• How to: set up an Override Account: Global Group
or:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up an Override Account: Group profile

IMPORTANT INFORMATION ABOUT USING THE ER IN THE EVALUATION MODE

When evaluating the ER and using this product in the evaluation mode, the Expiration screen in the Administrator console and the ER Server Statistics window in the client will display and function differently than they do in the activated (standard) mode of the ER (described in the ER Administrator User Guide and ER Web Client User Guide).

Administrator Console, Expiration Screen

On the Expiration screen, the following message displays at the top of the screen: “Evaluation Mode – Max Data Storage ‘X’ Weeks” (in which ‘X’ represents the maximum number of weeks in the ER’s data storage scope). In the evaluation mode, you will not be able to make adjustments to the data storage scope. Thus, the Save button is not included at the bottom of the screen. Evaluation Mode information is for viewing purposes only.


Database - Expiration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.101.76:88/process/expire.cgi
Go Links
8e6 Enterprise Reporter
Network
Server
Database
Logout
Help
Done
Internet

Expiration

Status as of 2007-11-13 13:04:40

EVALUATION MODE - MAX DATA STORAGE 24 WEEKS

Please click here to activate the box

Date scope for total data	2007-08-01 00:00:11 - 2007-11-13 12:59:59
Total number of week(s) stored	15 week(s)
Current live data (yearweekno/date scope)	200732 - 200745 2007-08-15 00:00:00 - 2007-11-13 12:59:59
Total number of live week(s)	13 week(s)
Current archive data (yearweekno/date scope)	200730 - 200732 2007-08-01 00:00:11 - 2007-08-14 23:59:59
Total number of archive week(s)	2 week(s)
Database disk space utilization (used database space/total database space)	13.79 % (5.78/41.94 Gbytes)
Target percentage of live data	90 %
Last 8 weeks hits/day average	130827
Estimated total week(s) of live data	24 week(s)
Estimated total week(s) of archive data	3 week(s)
Estimated number of week(s) until next expiration	0 week(s)

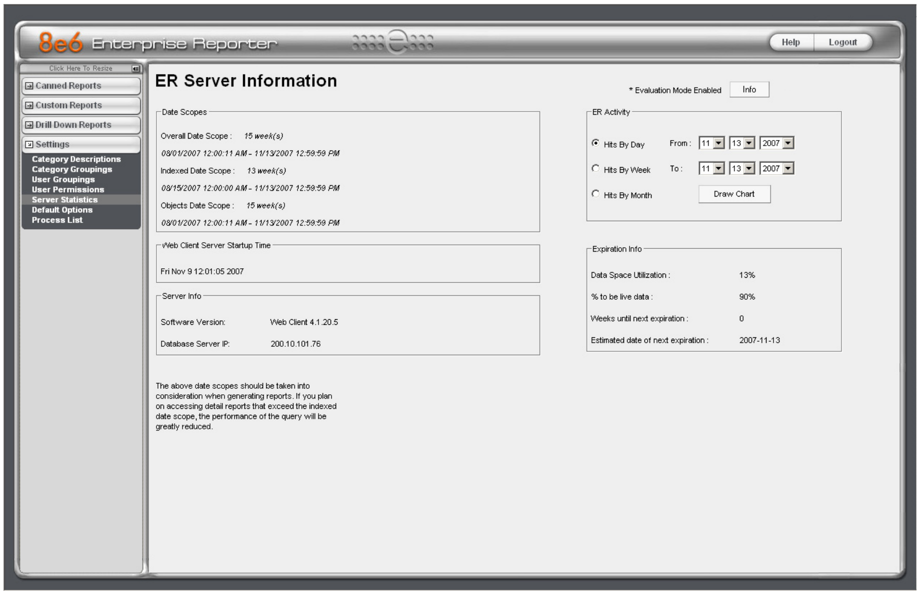
Change Settings

Hits/day	130827
Percentage of live data	90 %
Estimated total week(s) of live data	week(s)
Estimated total week(s) of archive data	week(s)

Calculate

ER Client, ER Server Statistics Window

In the ER Server Statistics window, the note "*Evaluation Mode Enabled" displays above the ER Activity frame. To the right of this note, the Info button displays. When this button is clicked, an alert box opens with the message: "Evaluation Mode – Max Data Storage 'X' Weeks" (in which 'X' represents the maximum number of weeks in the ER's data storage scope). Click OK to close the alert box.


8e6 Enterprise Reporter
Help
Logout
Click Here To Resize
Canned Reports
Custom Reports
Drill Down Reports
Settings
Category Descriptions
Category Groupings
User Groupings
User Permissions
Server Statistics
Default Options
Process List
Info
Draw Chart

ER Server Information

* Evaluation Mode Enabled

Date Scopes

Overall Date Scope : 15 week(s)
08/01/2007 12:00:11 AM - 11/13/2007 12:59:59 PM
Indexed Date Scope : 13 week(s)
08/15/2007 12:00:00 AM - 11/13/2007 12:59:59 PM
Objects Date Scope : 15 week(s)
08/01/2007 12:00:11 AM - 11/13/2007 12:59:59 PM

Web Client Server Startup Time

Fri Nov 9 12:01:05 2007

Server Info

Software Version: Web Client 4.1.20.5
Database Server IP: 200.10.101.76

The above date scopes should be taken into consideration when generating reports. If you plan on accessing detail reports that exceed the indexed date scope, the performance of the query will be greatly reduced.

ER Activity

● Hits By Day From : 11 13 2007
○ Hits By Week To : 11 13 2007
○ Hits By Month

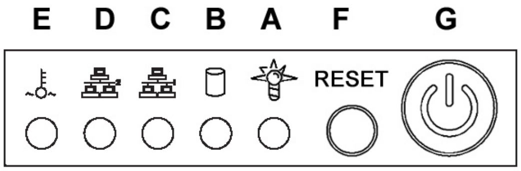
Expiration Info

Data Space Utilization : 13%
% to be live data : 90%
Weeks until next expiration : 0
Estimated date of next expiration : 2007-11-13

LED INDICATORS AND BUTTONS

Diagrams and Descriptions

LED indicators and buttons for hardware status monitoring display on the front panel, located on the right side of the chassis (see diagram below).



Chassis control panel

LED Indicator Key

A = Power
B = HDD Activity
C = LAN 1
D = LAN 2
E = Overheat

Button Key

F = Reset
G = Power

LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

LED Indicator	Color	Condition	Description
Power	Green	On	System On
		Off	System Off
HDD	Amber	Blinking	HDD Activity
		Off	No HDD Activity
LAN 1 & LAN 2	Green	On	Link Connected
		Blinking	LAN Activity
		Off	Disconnected
Overheat	Red	On	System Overheated
		Off	System Normal

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

USA:	UL 60950-1 2nd ed. 2007
Europe:	Low Voltage Directive (LVD) 2006/95/EC to CB Scheme EN 60950: 2006
International:	UL/CB to IEC 60950-1:2006

Electromagnetic Compatibility (EMC)

USA:	FCC CFR 47 Part 15, Verified Class A Limit
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 2004/108/EC & Low Voltage Directive (LVD) 2006/95/EC
Taiwan:	Bureau of Standards and Metrology Inspection (BSMI) CNS 13438: 2006

Federal Communications Commission (FCC) Class A Notice (USA)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Declaration of Conformity

Models: MSA-002-003

Electromagnetic Compatibility Class A Notice

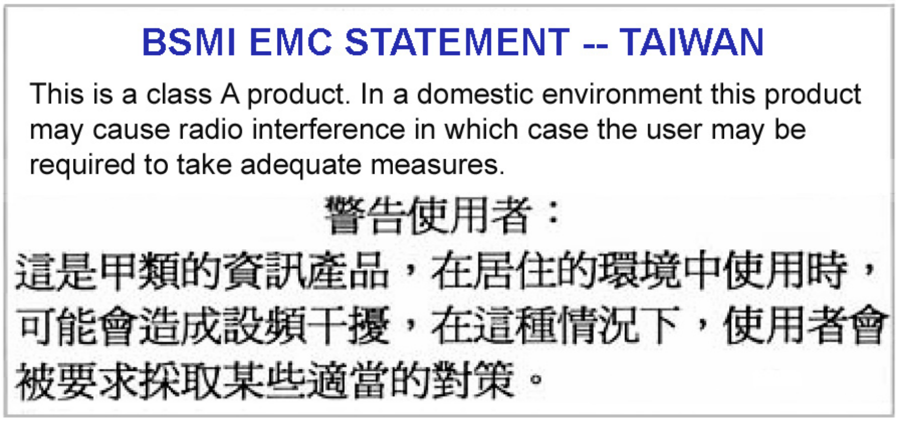
Industry Canada Equipment Standard for Digital Equipment (ICES-003)

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sure le matériel brouilleur du Canada.

English translation of the notice above:

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Bureau of Standards Metrology and Inspection (BSMI) - Taiwan



BSMI EMC STATEMENT -- TAIWAN

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成設頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

EC Declaration of Conformity

European Community Directives Requirement (CE)

Declaration of Conformity

Manufacturer's Name: 8e6 Technologies
Manufacturer's Address: 828 W. Taft Avenue
Orange, CA 92865

Application of Council Directive(s):
Low Voltage • 2006/95/EC
EMC • 2004/108/EC

Standard(s):
Safety • EN60950: 2006

EMC
- EN55022: 2006
- EN55024: 1998 +A2:2003
- EN61000-3-2: 2000
- EN61000-3-3: 2001

Product Name(s): Internet Appliance

Product Model Number(s): MSA-002-003

Year in which conformity is declared: 2008

All hardware components supplied in this unit's shipping carton are certified by our vendors to be RoHS compliant.

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

Location: Orange, CA, USA
Signature:

Date: January 21, 2008
Full Name: Gregory P. Smith
Position: Director of Engineering Operations

INDEX

A

Always Allow Custom Category 69

B

Bandwidth/Productivity 59
boot up 31
BSMI 74, 75

C

Category block 55, 63
Change Quick Start password 27
Change User Name and Password 48
crossover cable 20, 30, 40
Custom Block/Warn/X Strikes/Quota pages 65, 68
Custom Category (blocked) 57
Customize an 8e6 Supplied Category 68
Custom Lock, Block, Warn, X Strikes, Quota pages 56

E

EMC 74, 76
ER Client 51, 72
ER Server Statistics 71, 72
Evaluation Mode 2, 71, 72
Exception URL bypass 58
Expiration 71

F

FCC 74
File type blocking 59
Filtering Scenarios 55

G

Game patterns 62
General/Productivity 66

H

HTTPS settings 63
HyperTerminal Setup 22

I

ICES-003 74, 75
IM patterns 62
IP exceptions 69

L

Local category adds/deletes 68
Login screen 25
LVD 74

M

Minimum Filtering Level 57

O

Overall Quota 60, 67
Overheat 73
Override Account bypass 58
Override Accounts 70

P

P2P patterns 61
Pass/Allow 69
Physically Connect the R3000IR to the Network 40
Power Supply Precautions 16
Proxy Patterns 58

Q

Quick Start menu 25

R

Rack Setup Precautions 7
Real Time Probe information 65
reboot 34, 39, 40
Remote Access patterns 63
Reset admin console account 27
Reset system to factory defaults 27
RoHS compliant 76
Rule block 55, 64

S

Search Engine Keywords 57
SE Keywords 64
serial port cable 5, 20, 21
shut down 40
Streaming Media patterns 62

T

Threat Class Groups 54
Threats/Liabilities 55
Time Based Profiles 60, 67
Time Quota/Hit Quota 59, 67

U

UL 74
URL exceptions 69
URL Keywords 56, 64

W

Warn-strike 61
Warn-strike with higher thresholds 66
Warn Feature with higher thresholds 66
Warn option with low filter settings 60

X

X-Strike on blocked categories 55

8e6 Corporate Headquarters (USA):
828 West Taft Avenue Orange, CA 92865-4232 • Tel: 714.282.6111 or 888.786.7999
Fax: 714.282.6116 (Sales/Technical Support) • 714.282.6117 (General Office)

Satellite Office:
8e6 Taiwan: 7 Fl., No. 1, Sec. 2, Ren-Ai Rd., Taipei 10055, Taiwan, R.O.C.
Tel: 886-2-2397-0300 • Fax: 886-2-2397-0306